

## Procesadores IA-32 e Intel® 64

### Gestión de Memoria

Alejandro Furfaro

8 de abril de 2020

# Temario

- 1 Administración de memoria
  - Enfoque preliminar
  - Gestión de la Memoria
- 2 Como se organiza la memoria en procesadores x86
  - Modelo de memoria en Modo Protegido
  - Modelo de memoria en Modo 64 bits
- 3 Direcciones Lógicas y Lineales
  - Traducción de direcciones Lógicas
- 4 Unidad de Segmentación
  - Selectores de segmento
  - Descriptores de segmento de 32 bits
- 5 Generación de la dirección Lineal (32 bits)
- 6 Modelos de segmentación de memoria

- 7 Segmentación en Modo IA-32e
  - Implementación práctica de segmentación en un SO
- 8 Paginación
  - Introducción
  - Unidad de Paginación - IA32
  - Paginación en IA-32 (32 bits)
  - Formatos de descriptores de página
  - Paginación PAE
  - Paginación IA-32e
  - Niveles vs. Modos de paginación
- 9 Paginación en ARMv7 Cortex-A y Cortex-R
  - Introducción
  - Memory Management Unit
- 9 Paginación en un Sistema Operativo Real: Linux

- 1 Administración de memoria
  - Enfoque preliminar
  - Gestión de la Memoria
- 2 Como se organiza la memoria en procesadores x86
  - Modelo de memoria en Modo Protegido
  - Modelo de memoria en Modo 64 bits
- 3 Direcciones Lógicas y Lineales
  - Traducción de direcciones Lógicas
- 4 Unidad de Segmentación
  - Selectores de segmento
  - Descriptores de segmento de 32 bits
- 5 Generación de la dirección Lineal (32 bits)
- 6 Modelos de segmentación de memoria



- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

- 7 Paginación
  - Introducción
  - Unidad de Paginación - IA32
  - Paginación en IA-32 (32 bits)
  - Formatos de descriptores de página
  - Paginación PAE
  - Paginación IA-32e
  - Niveles vs. Modos de paginación
- 8 Paginación en ARMv7 Cortex-A y Cortex-R
  - Introducción
  - Memory Management Unit
- 9 Paginación en un Sistema Operativo Real: Linux

# Dirección Lógica, Virtual, Física.... ¿?

- ¿Como es que hay diferentes definiciones de direcciones?. ¿No son todas lo mismo?
- No siempre.
- En los microcontroladores sencillos o de arquitecturas muy primitivas, estos conceptos significan lo mismo
- Pero a medida que los procesadores ganan complejidad en su arquitectura, y soportan mayor grado de funcionalidades y aspiran a sostener Sistemas Operativos con ejecución dinámica de tareas, estos tres valores suelen ser diferentes.



# Dirección Física

- Cuando cualquier procesador necesita acceder a memoria, deberá escribir en el buffer de direcciones el valor correspondiente a la dirección de memoria externa que debe acceder.
- Este valor se conoce como Dirección Física, ya que corresponde a la dirección que será decodificada por el hardware externo para acceder a la memoria RAM o ROM según corresponda. Es decir a la memoria física.
- Siempre el procesador pone la Dirección Física en los pines de address cuando su unidad de control habilita la salida del bus de direcciones



# ¿Que dirección manejamos en los programas?

- El texto de nuestros programas fuente provee implícitamente una visión mas o menos abstracta de la memoria.
- En mayor o menor medida intentamos abstraernos del valor numérico de la dirección, aun cuando programamos los procesadores mas rudimentarios

---

```
1 buffer resb 1024 db      ; define 1024 bytes de memoria en 0
2 .....
3 mov al,00      ; valor inicial
4 mov ecx,1024    ; inicializa contador en 1024
5 mov esi,buffer  ; guarda en esi la dirección de memoria de buffer
6 repnz stosb    ; Accede al buffer y lo inicializa
```

---

En este código se define un buffer de 1024 bytes.

- ¿Cual es su dirección de Memoria?



# Dirección Lógica

## Definición

- Es la dirección de memoria expresada en términos abstractos por el programador en su código fuente.
- Es una forma muy simple de trabajar en forma transparente a la memoria.
- En lugar de referirse al valor numérico de la dirección de hardware, reemplazamos este valor por una etiqueta que incluso resulte ilustrativa de lo que representa esa dirección, y dejamos que el toolchain resuelva su valor numérico.



# ¿Qué es la dirección virtual?

- Generalmente coincide con la dirección lógica (Aun en procesadores de alta gama).
- Sin embargo, en algunos procesadores las direcciones lógica y la virtual son diferentes.
- Inclusive encontraremos que se refieren a ella como dirección lineal.



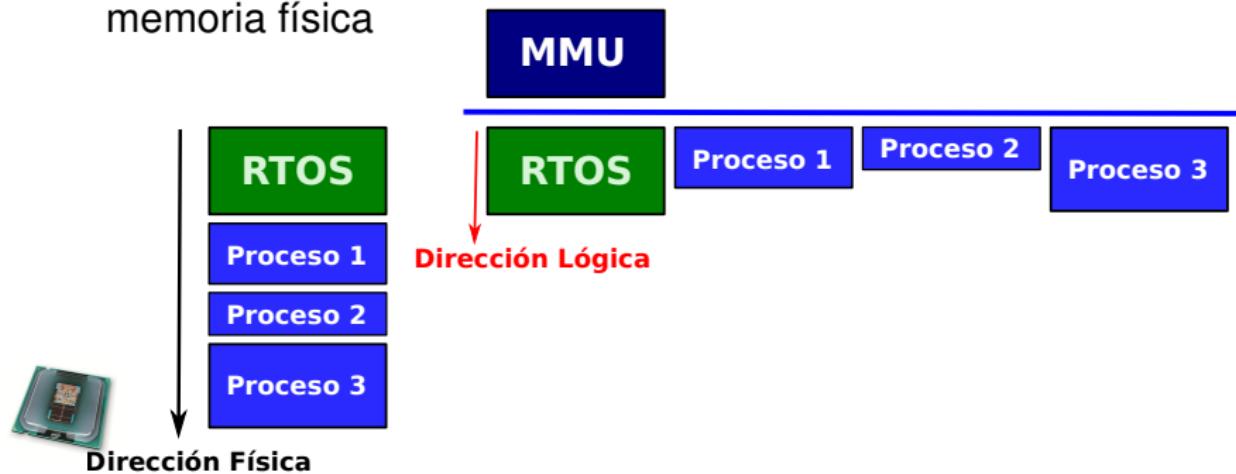
- 1 Administración de memoria
  - Enfoque preliminar
  - Gestión de la Memoria
- 2 Como se organiza la memoria en procesadores x86
  - Modelo de memoria en Modo Protegido
  - Modelo de memoria en Modo 64 bits
- 3 Direcciones Lógicas y Lineales
  - Traducción de direcciones Lógicas
- 4 Unidad de Segmentación
  - Selectores de segmento
  - Descriptores de segmento de 32 bits
- 5 Generación de la dirección Lineal (32 bits)
- 6 Modelos de segmentación de memoria

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

- 7 Paginación
  - Introducción
  - Unidad de Paginación - IA32
  - Paginación en IA-32 (32 bits)
  - Formatos de descriptores de página
  - Paginación PAE
  - Paginación IA-32e
  - Niveles vs. Modos de paginación
- 8 Paginación en ARMv7 Cortex-A y Cortex-R
  - Introducción
  - Memory Management Unit
- 9 Paginación en un Sistema Operativo Real: Linux

# Memory Management Unit

- La MMU cambia el mapeo entre una Dirección Lógica y la Dirección Física.
- Provee una visión de la memoria física, dividida en fragmentos para su mejor administración.
- Permite al Sistema Operativo asignar el mismo espacio de direcciones lógicas para los procesos, separándolos en la memoria física



# Una MMU hace la diferencia

- La MMU es fundamental para implementar el modelo de proceso en un Sistema Operativo (como es el caso de Linux).
- En este caso cada tarea tiene una o mas áreas de memoria para su código y datos.
- Cuando el scheduler retoma la ejecución de una tarea, la MMU mapea su espacio de direccionamiento lógico (que comienza en 0) en un área de memoria física exclusiva y diferente de la de las demás tareas y del propio Sistema Operativo.
- De este modo cada tarea (proceso) gana su espacio de memoria físico exclusivo y queda protegido el del resto de las tareas (procesos).
- La desventaja es el overhead que genera remapear la memoria cada vez que se conmuta de un proceso al siguiente.
- La MMU asegura a cada tarea (proceso), la visibilidad de su propia área de memoria, y de las partes relevantes del sistema operativo.

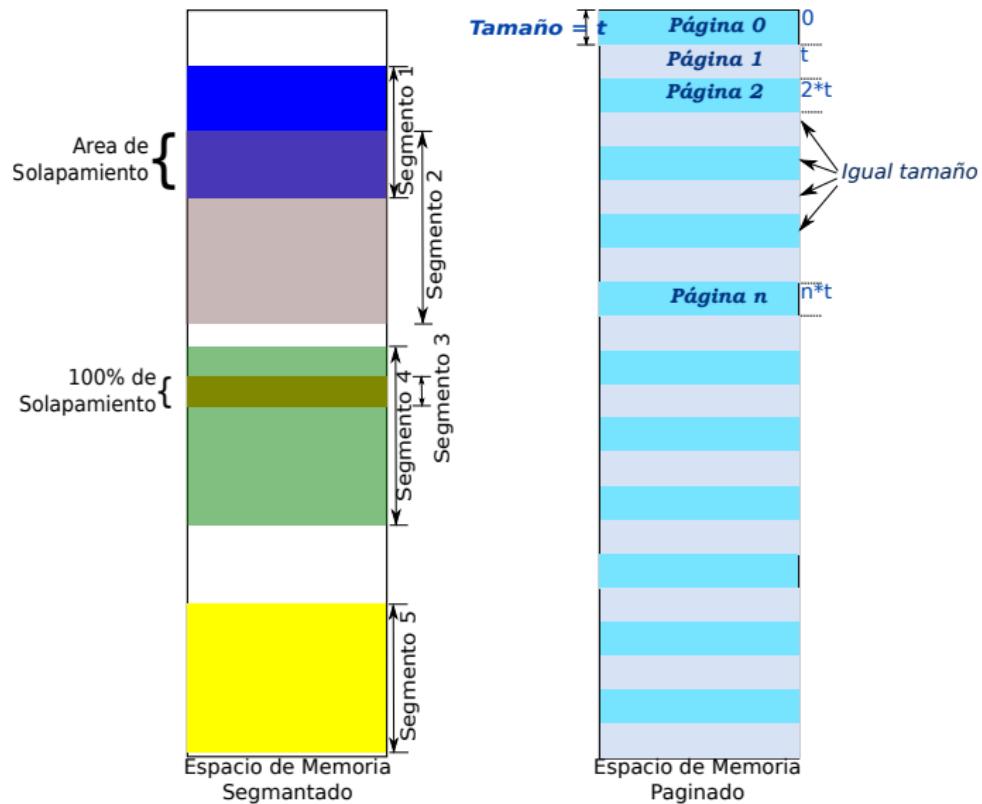


# Administración de Memoria con MMU

- La división de la memoria en bloques, se puede realizar mediante dos criterios diferentes
  - Paginación.
  - Segmentación.
- O en algunos casos como una combinación o superposición de ambos.



# Segmentación vs. Paginación



# Espacio Físico

- Los procesadores IA-32 organizan la memoria como una secuencia de bytes, direccionables a través de su Bus de Address.
- La memoria conectada a este bus se denomina **memoria física**.
- El espacio de direcciones que pueden volcarse sobre este bus se denomina **direcciones físicas**.

## Capacidad de direccionamiento de memoria

Los procesadores IA-32 son la continuación del 8086. Este procesador fue el primer de 16 bits de ancho de palabra, y por ende todos sus registros internos tienen ese tamaño. Su espacio de Direccionamiento es de 1 Mbyte ∵ Address Bus es de 20 líneas. Este espacio de direccionamiento se administra por segmentación.

# Espacio Lógico

## Segmentación

Por diversos motivos que en su momento tuvieron sentido, Intel definió organizar el espacio de direccionamiento de la Familia iAPx86 en segmentos. El compromiso de compatibilidad ató a los siguientes procesadores a mantener este esquema

## Condiciones iniciales de segmentación

- 4 registros de segmento para almacenar hasta 4 selectores de segmento.
- Registros de 16 bits los segmentos tienen a lo sumo 64K de tamaño
- Expresión de las direcciones en el modelo de programación mediante dos valores:
  - ① Identificador del segmento en el que se encuentra la variable o la instrucción que se desea direccionar,
  - ② Desplazamiento, offset, o **dirección efectiva** a partir del inicio de ese segmento en donde se encuentra efectivamente

# Espacio Lógico



- Estos dos valores por si solos no tienen significado físico
- Para lograr a partir de ellos identificar la **dirección física** de la variable o instrucción el procesador debe realizar una serie de operaciones.

## Dirección Lógica

A una dirección de memoria expresada en términos de los recursos de la arquitectura del procesador las llamaremos **dirección lógica**.

**1 Administración de memoria**

- Enfoque preliminar
- Gestión de la Memoria

**2 Como se organiza la memoria en procesadores x86**

- **Modelo de memoria en Modo Protegido**
- Modelo de memoria en Modo 64 bits

**3 Direcciones Lógicas y Lineales**

- Traducción de direcciones Lógicas

**4 Unidad de Segmentación**

- Selectores de segmento
- Descriptores de segmento de 32 bits

**5 Generación de la dirección Lineal (32 bits)****6 Modelos de segmentación de memoria**

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

**7 Paginación**

- Introducción
- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)
- Formatos de descriptores de página
- Paginación PAE
- Paginación IA-32e
- Niveles vs. Modos de paginación

**8 Paginación en ARMv7 Cortex-A y Cortex-R**

- Introducción
- Memory Management Unit

**9 Paginación en un Sistema Operativo Real: Linux**

# Origen y Evolución

- Con el procesador 80286 se incluyó (aún en un procesador de 16 bits) un nuevo modo de trabajo que evolucionaría con la arquitectura IA-32: El Modo Protegido.
- Aún con la aparición de las extensiones de 64 bits para esta familia de procesadores, este modo de trabajo no ha caído en desuso.
- Sin embargo es de esperar que en algún momento todo pase a funcionar en 64 bits. Nos referiremos a éste modo como el Modo Legacy.
- Desde el 80386 en adelante los procesadores de Intel vienen provistos de 32 líneas de datos y 32 líneas independientes de address. Esto hace que cualquier procesador IA-32 direcciona  $2^{32} - 1$  bytes.
- A partir de la microarquitectura P6 se incluyeron cuatro líneas adicionales en el bus de address las cuales se habilitan desde modo protegido siempre que se haya activado la paginación. De este modo se llega a  $2^{36} - 1$  bytes (64 Gbytes de **memoria física**)



**1 Administración de memoria**

- Enfoque preliminar
- Gestión de la Memoria

**2 Como se organiza la memoria en procesadores x86**

- Modelo de memoria en Modo Protegido

**3 Direcciones Lógicas y Lineales**

- Traducción de direcciones Lógicas

**4 Unidad de Segmentación**

- Selectores de segmento
- Descriptores de segmento de 32 bits

**5 Generación de la dirección Lineal (32 bits)****6 Modelos de segmentación de memoria**

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

**7 Paginación**

- Introducción
- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)
- Formatos de descriptores de página
- Paginación PAE
- Paginación IA-32e
- Niveles vs. Modos de paginación

**8 Paginación en ARMv7 Cortex-A y Cortex-R**

- Introducción
- Memory Management Unit

**9 Paginación en un Sistema Operativo Real: Linux**

# Particularidades

- Como hemos visto, se puede ingresar a un modo denominado IA-32e, en el que se trabaja con una arquitectura de 64 bits
  - En este modo se generan direcciones lineales de 64 bits, de los que por el momento se utilizan los 48 menos significativos.
  - En realidad la cantidad de bits significativos de la dirección lineal es procesador dependiente y se puede determinar mediante la función 0x80000008 de la instrucción CPUID (vuelve en AH).
  - Una **dirección lineal** tiene formato canónico, cuando sus bits desde el 63 al mas significativo de los válidos devueltos por la instrucción CPUID.80000008H están todos en el mismo estado que el bit mas significativo. Al momento esta función retorna 48 para todos los procesadores, de modo que una **dirección lineal** tiene formato canónico si los bits 48 a 63 están el mismo estado lógico que el bit 47.
-  Por cada acceso a memoria en el modo IA-32e submodo 64 bits, la unidad de protección del procesador chequea el formato canónico de la **dirección lineal**.

# Formato Canónico

Si no está en formato canónico...excepción!

Generalmente la excepción es de protección general #GP, excepto en el caso que la dirección se genere a partir de una dirección que haga referencia a la pila, y que por lo tanto se calcula a partir del stack segment, en cuyo caso se genera una excepción de pila #SF.

Por lo general las instrucciones que la generan son PUSH, POP, y referencias a memoria que utilicen RSP y RBP, excepto si estas instrucciones utilizan un prefijo de segmento FS o GS que pise el valor default, en cuyo caso generarían una excepción #GP (Notar que los prefijos de segmento DS ES y CS se ignoran en modo 64 bits).



**1 Administración de memoria**

- Enfoque preliminar
- Gestión de la Memoria

**2 Como se organiza la memoria en procesadores x86**

- Modelo de memoria en Modo Protegido
- Modelo de memoria en Modo 64 bits

**3 Direcciones Lógicas y Lineales****● Traducción de direcciones Lógicas****4 Unidad de Segmentación**

- Selectores de segmento
- Descriptores de segmento de 32 bits

**5 Generación de la dirección Lineal (32 bits)****6 Modelos de segmentación de memoria**

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

**7 Paginación**

- Introducción
- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)
- Formatos de descriptores de página
- Paginación PAE
- Paginación IA-32e
- Niveles vs. Modos de paginación

**8 Paginación en ARMv7 Cortex-A y Cortex-R**

- Introducción
- Memory Management Unit

**9 Paginación en un Sistema Operativo Real: Linux**

# Traducción de direcciones

Estos procesadores en Modo Protegido generan una **dirección física** en el bus de address mediante un proceso de traducción en dos niveles:

- ① traslación de una dirección lógica
- ② paginación del espacio lineal

## La MMU

El procesador posee una MMU (Memory Management Unit) compuesta de dos subunidades conectadas en cascada: La Unidad de Segmentación que se encarga de trasladar la **dirección lógica** en una **dirección lineal**, y la Unidad de Página que traduce la **dirección lineal** en una **dirección física** que enviará por el bus de address hacia la memoria externa.

# El espacio Lineal

## Definición

El espacio lineal de direcciones es al igual que el espacio físico un rango de direcciones contiguas plano, que inicia en la dirección 0, y llega al máximo valor que puede ocupar un segmento de acuerdo al modo de trabajo. Por ejemplo en modo protegido de 32 bits el rango de direcciones lineales arranca en 0 y puede llegar hasta  $2^{32} - 1$ , es decir 0xFFFFFFFF. En el modo 64 bits la dirección lógica resultante es de 64 bits y debe estar representada en formato canónico.



# Traslación de la dirección lógica

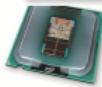
- El procesador debe tener la capacidad de especificar a cada proceso o tarea, donde comienza cada uno de sus segmentos y cual es su tamaño.
- La dirección de comienzo de un segmento es un valor de 32 bits en modo protegido.
- El tamaño máximo que puede tener un segmento es el de su máximo valor de desplazamiento, este valor también es de 32 bits en modo protegido y hasta el momento 48 bits en modo IA-32e.
- Además es lógico pensar que se necesiten algunos bits adicionales de control para administración de acceso a los diferentes segmentos.



# Traslación de la dirección lógica

## Conclusión

Los modestos 16 bits de un registro de segmento resultan absolutamente insuficientes para almacenar toda esta información. todo lo que puede contener un registro de segmento es un valor, que como ya se ha dicho, se denomina selector de segmento, y que no es otra cosa que una referencia a una estructura de datos mas grande que contiene, la **Dirección Base**, el **Límite**, y los **Atributos** del segmento seleccionado. Como veremos esta estructura se denomina **Descriptor de Segmento**, reside en la memoria RAM del sistema, y para mejor organización se los agrupa en tablas, de modo de facilitar su ubicación al procesador mediante un mecanismo predeterminado.



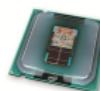
- 1 Administración de memoria
  - Enfoque preliminar
  - Gestión de la Memoria
- 2 Como se organiza la memoria en procesadores x86
  - Modelo de memoria en Modo Protegido
  - Modelo de memoria en Modo 64 bits
- 3 Direcciones Lógicas y Lineales
  - Traducción de direcciones Lógicas
- 4 Unidad de Segmentación
  - Selectores de segmento
  - Descriptores de segmento de 32 bits
- 5 Generación de la dirección Lineal (32 bits)
- 6 Modelos de segmentación de memoria
- 7 Paginación
  - Introducción
  - Unidad de Paginación - IA32
  - Paginación en IA-32 (32 bits)
  - Formatos de descriptores de página
  - Paginación PAE
  - Paginación IA-32e
  - Niveles vs. Modos de paginación
- 8 Paginación en ARMv7 Cortex-A y Cortex-R
  - Introducción
  - Memory Management Unit
- 9 Paginación en un Sistema Operativo Real: Linux



# Formato



- **Index.** Se utiliza como índice en la tabla de descriptores. Un valor de **Index** =  $n$ , corresponde al  $n$ -ésimo elemento de la Tabla. Al tener 13 bits indica que cada tabla puede alojar  $2^{13}$  (8192) descriptores.
- **TI.** Table Indicator. Selecciona en que tabla de descriptores debe buscarse el segmento seleccionado: **GDT** por Global Descriptor Table (si **TI** = 0), o **LDT** por Local Descriptor Table (Si **TI** = 1).
- **RPL** Requested Priviledge Level. En el Capítulo Protección lo abordaremos en detalle. Por ahora solo interesa saber que este campo es el nivel de privilegio que declara tener el dueño del segmento, o sea el grado de autorización que se tiene para cada acceso: 00 es el mayor privilegio, y 11 el menor.



**1 Administración de memoria**

- Enfoque preliminar
- Gestión de la Memoria

**2 Como se organiza la memoria en procesadores x86**

- Modelo de memoria en Modo Protegido
- Modelo de memoria en Modo 64 bits

**3 Direcciones Lógicas y Lineales**

- Traducción de direcciones Lógicas

**4 Unidad de Segmentación**

- Selectores de segmento
- **Descriptoros de segmento de 32 bits**

**5 Generación de la dirección Lineal (32 bits)****6 Modelos de segmentación de memoria**

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

**7 Paginación**

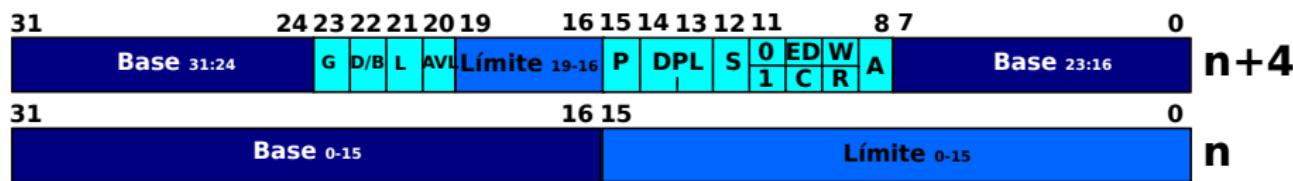
- Introducción
- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)
- Formatos de descriptoros de página
- Paginación PAE
- Paginación IA-32e
- Niveles vs. Modos de paginación

**8 Paginación en ARMv7 Cortex-A y Cortex-R**

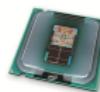
- Introducción
- Memory Management Unit

**9 Paginación en un Sistema Operativo Real: Linux**

# Formato



- **Dirección Base** . Es la dirección a partir de la cual se despliega en forma continua el segmento.
- **Límite** . El Límite de un segmento especifica el máximo offset que puede tener un byte direccionable dentro del segmento. Suele confundirse este concepto con el tamaño del segmento. En realidad el **Límite** es el tamaño del segmento menos 1, ya que el offset del primer byte del segmento es 0.



# Atributos

- **G.** Granularity. Establece la unidad de medida del campo **Límite**. Si **G** = 0, el máximo offset de un byte es igual a **Límite**. Si **G** = 1, el máximo offset es igual a **Límite** \* 0x1000 +0xFFFF.
- **D/B.** Default / Big. Configura el tamaño de los segmentos. Si es 0, (Default) el segmento es de 16 bits. Si es 1, (Big) es un segmento de 32 bits. Para segmentos de código, **D/B** = 0 implica que el tamaño de datos es de 16 bits u 8 bits, y el de direcciones de 16 bits. Si en cambio **D/B** = 1, el tamaño de un offset es 32 bits y el de los operandos es de 32 bits u 8 bits. En ambos casos mediante los prefijos de instrucción 66h y 67h respectivamente podemos alterar los defaults. En el caso de un segmento de datos utilizado como pila, si **D/B** = 0 las operaciones de la pila son de 16 bits, aunque el operando de la instrucción sea de 8 bits. Si **D/B** = 1, son de 32 bits independientemente del tamaño del operando. El valor tope del segmento será también consecuencia del valor de este bit.



# Atributos

- **L.** El procesador solo mira este bit en el Modo IA-32e. Si en un segmento de código este bit es '1', indica que el segmento contiene código nativo de 64 bits, caso contrario, ejecutará en Modo Compatibilidad. En modo IA-32e, si **L** es '1', entonces **D/B** debe estar en '0'. Si el procesador no está en modo IA-32e, o si está en este modo pero el segmento no es de código, el bit **L** debe estar siempre en '0'.
- **AVL.** **AVaiLable**. Este bit no es usado por el procesador para ningún propósito específico. Queda para que el programador de sistemas le asigne el uso que considere mas apropiado.
- **P.** **Present**. Cuando es '1' el segmento correspondiente está presente en la memoria RAM. Si es '0', el segmento está en la memoria virtual (disco). Un acceso a un segmento cuyo bit **P** está en '0', genera una excepción #NP (Segmento No Presente). Esto permite al kernel solucionar el problema, efectuando el “swap” entre el disco a memoria para ponerlo accesible en RAM.



# Atributos

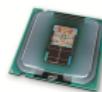
- **A.** Accedido. Se setea cada vez que se accede una dirección en el segmento. Permite al Sistema Operativo contabilizar los accesos para elaborar estadísticas de uso que permitan identificar cual es el segmento a ser desalojado llegado el momento.
- **DPL.** Descriptor Priviledge Level. Nivel de privilegio que debe tener el segmento que contiene el código que pretende acceder a éste segmento.
- **S.** System. Este bit, **activo bajo** permite administrar en las tablas de descriptoros, dos clases bien determinadas de segmentos:
  - 1 Segmentos de Código o Datos
  - 2 Segmentos de Sistema. Tienen diferentes formatos y en general no se refieren a zonas de memoria (salvo TSS). En general se refieren a mecanismos de uso de recursos del procesador por parte del kernel (por ello reciben el nombre de descriptoros de Sistema, ya que **son para uso exclusivo del Sistema Operativo**)



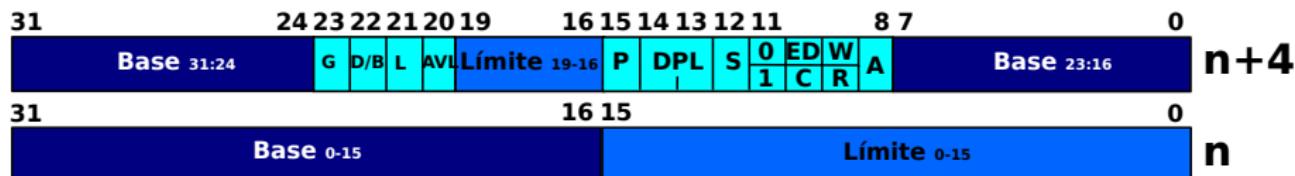
**Tipo.** Este campo de 4 bits es fuertemente dependiente del tipo (de allí el nombre, según se trate de un segmento de Código, de Datos o de Sistema). Su detalle se establece a continuación:

# Tipos de Descriptoros de Sistema ( $S = 0$ )

11	10	9	8	Modo 32 bits	Modo IA-32e
0	0	0	0	Reservado	8 bytes superiores en un segmento de 16 bytes
0	0	0	1	TSS de 16 bits disponible	Reservado
0	0	1	0	LDT	LDT
0	0	1	1	TSS de 16 bits Busy	Reservado
0	1	0	0	Call Gate de 16 bits	Reservado
0	1	0	1	Task Gate	Reservado
0	1	1	0	Interrupt Gate de 16 bits	Reservado
0	1	1	1	Trap Gate de 16 bits	Reservado
1	0	0	0	Reservado	Reservado
1	0	0	1	TSS de 32 bits disponible	TSS de 64 bits disponible
1	0	1	0	Reservado	Reservado
1	0	1	1	TSS de 32 bits Busy	TSS de 64 bits Busy
1	1	0	0	Call Gate de 32 bits	Call Gate de 64 bits
1	1	0	1	Reservado	Reservado
1	1	1	0	Interrupt Gate de 32 bits	Interrupt Gate de 64 bits
1	1	1	1	Trap Gate de 32 bits	Trap Gate de 64 bits



# Tipos de Descriptoros de Código y Datos (S = 1)



- En este caso el bit 11 define si el segmento correspondiente a este descriptor es de código o de datos según valga '1', o '0' respectivamente. En cada caso los dos bits subsiguientes tienen un significado diferente.
- Si el bit 11 es '1' el segmento es de código
- Si el bit 11 es '0' el segmento es de datos



# Atributos de Descriptores de Código( $S = 1$ , $Bit_{11} = 1$ )

- **C.** Conforming. Significa ajustable. Estos segmentos de código "ajustan" su nivel de privilegio al del código que los ha invocado. Permiten que un segmento de código pueda ser invocado desde otro segmento de código menos privilegiado mediante por ejemplo una instrucción CALL a una subrutina residente en este segmento. Sin embargo el código privilegiado ajustará su nivel de privilegio al del segmento de código invocante.
- **R.** Readable. Este bit habilita cuando es '1' la lectura de direcciones de memoria residente en el segmento. En general se usa cuando se tienen constantes en el segmento que necesitan ser accedidas para su lectura. Si el segmento solo tiene código, puede ponerse R = 0 en el descriptor para prevenir que se pueda leer cualquier ítem de este segmento utilizando el prefijo CS en la instrucción para modificar el comportamiento del procesador en la asignación por default del registro de segmento en el modo de direccionamiento empleado.



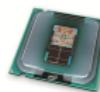
# Atributos de Descriptores de Datos( $S = 1$ , $Bit_{11} = 0$ )

- **ED.** Expand Down. Cuando el segmento de datos va a ser utilizado como Pila, puede optarse por tratarlo como un segmento común de datos, o definirlo como Expand Down, poniendo de manifiesto que es una pila, y su puntero de direcciones decrece hacia las direcciones de memoria numéricamente menores a medida que se expande el segmento (de allí el término Expand Down). En este caso, el concepto de límite efectivo se interpreta de modo diferente: Es el último valor de offset a partir de la dirección base que no puede ser accedido. Para estos segmentos el rango de offsets válidos es el siguiente:

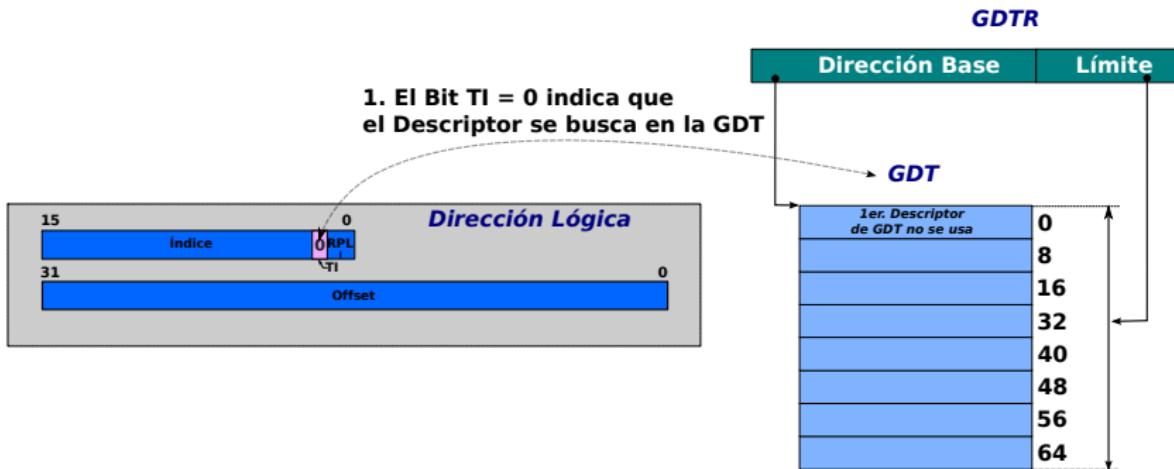
- (límite efectivo +1) hasta 0FFFFh, si el bit **D/B** = 0.
- (límite efectivo +1) hasta 0xFFFFFFFFh, si el bit **D/B** = 1.

Se ampliará al tocar el tema protección.

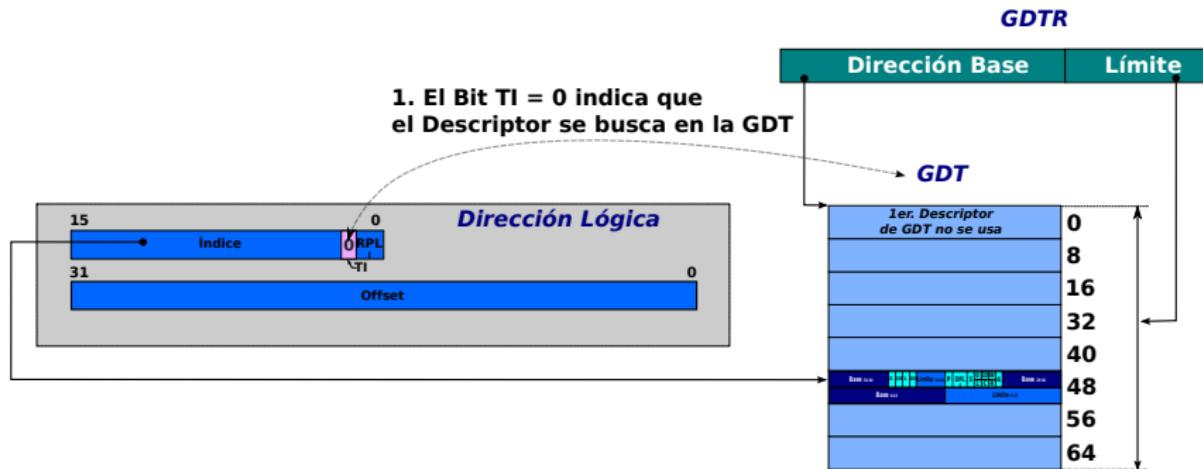
- **W.** Writable. Este bit, indica si el segmento de datos puede escribirse. Si este bit está en '0', el segmento contiene datos pero es Read Only.



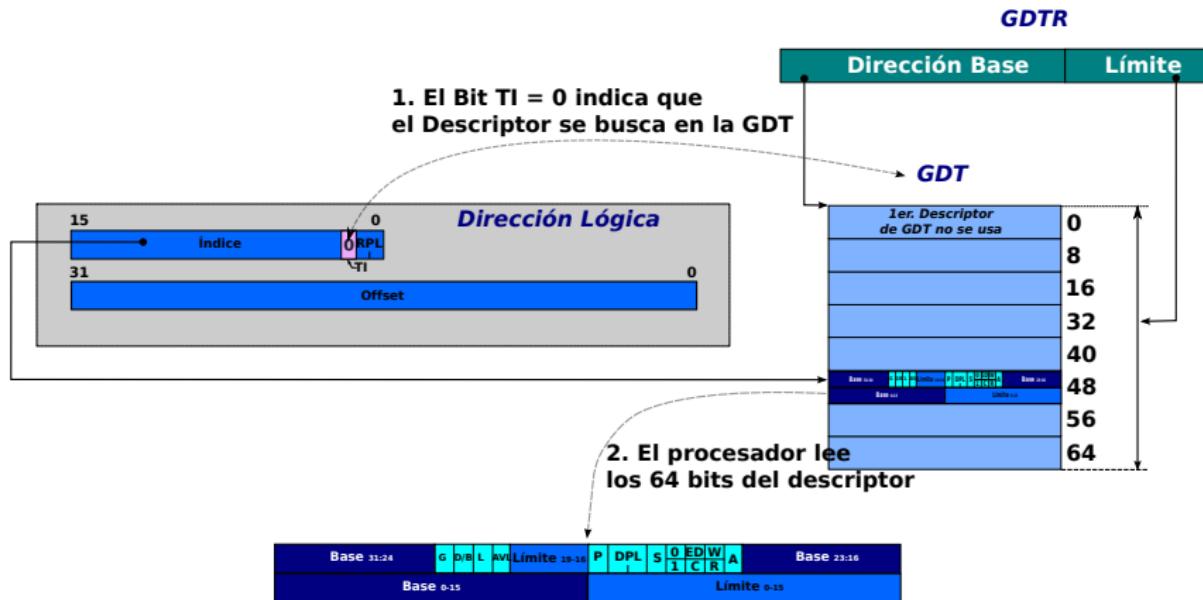
# Descriptoros de Segmento en la GDT (**TI = 0**)



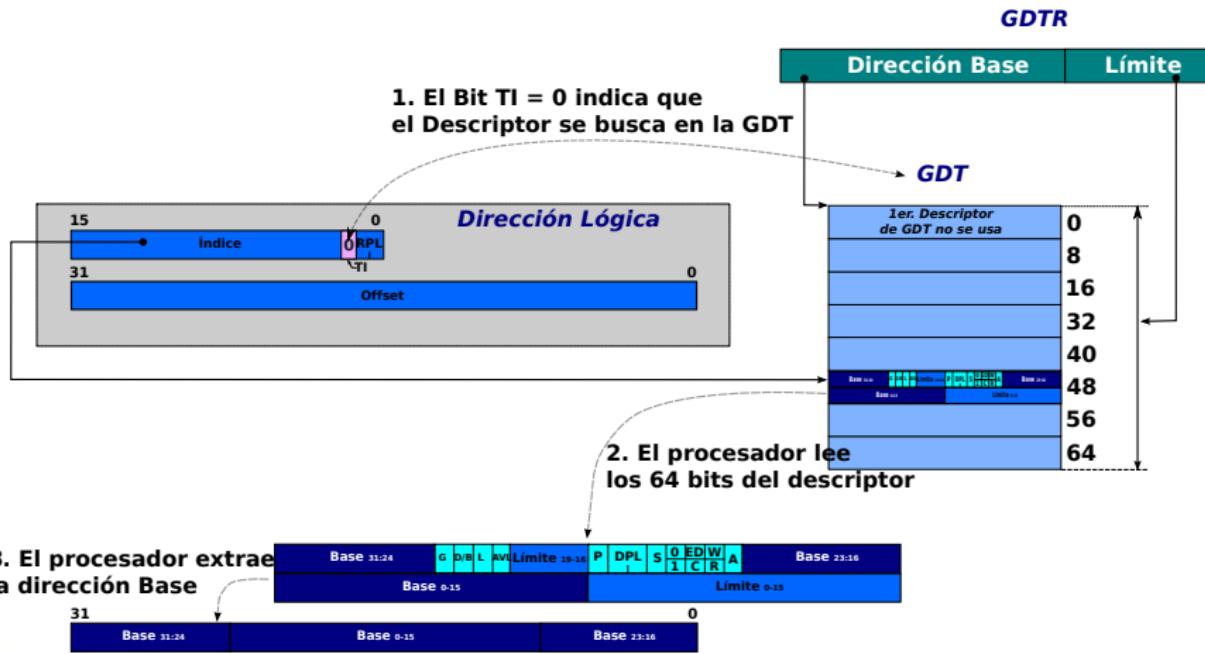
# Descriptoros de Segmento en la GDT (**TI** = 0)



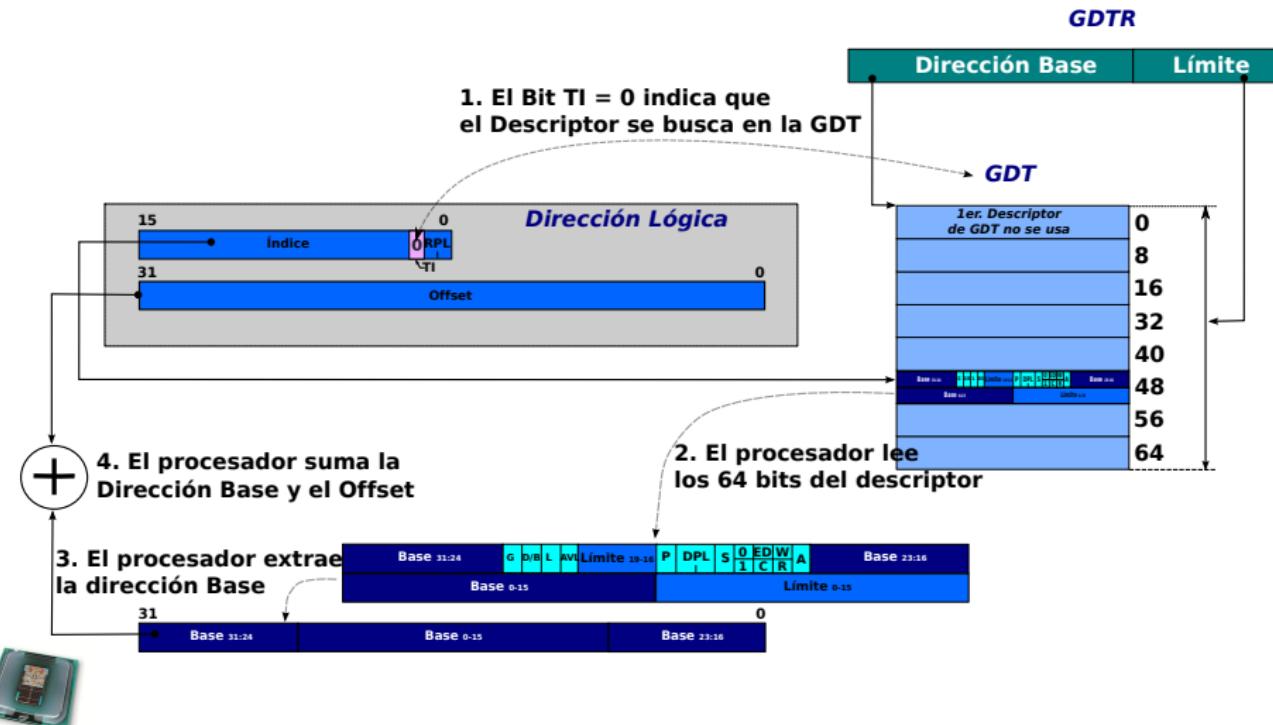
# Descriptoros de Segmento en la GDT (**TI** = 0)



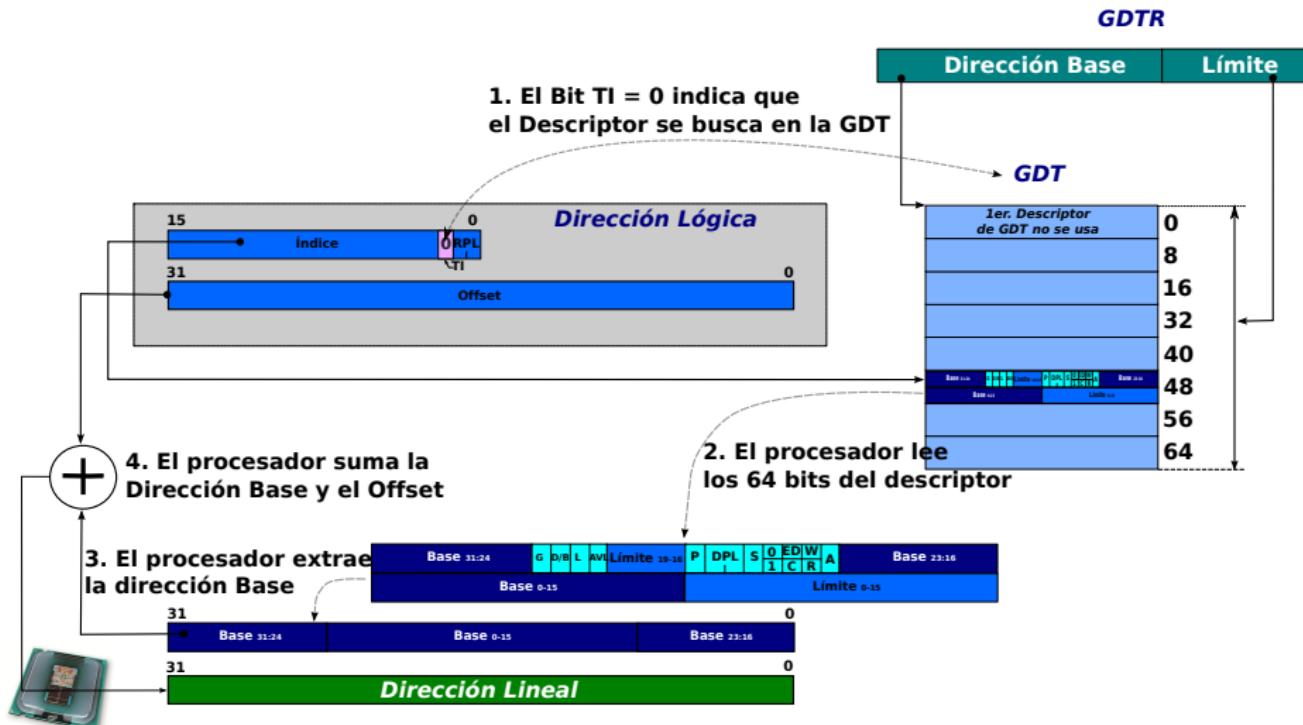
# Descriptoros de Segmento en la GDT (**TI** = 0)



# Descriptoros de Segmento en la GDT (**TI** = 0)



# Descriptoros de Segmento en la GDT (**TI = 0**)



# Descriptoros de Segmento en la GDT (**TI** = 0)

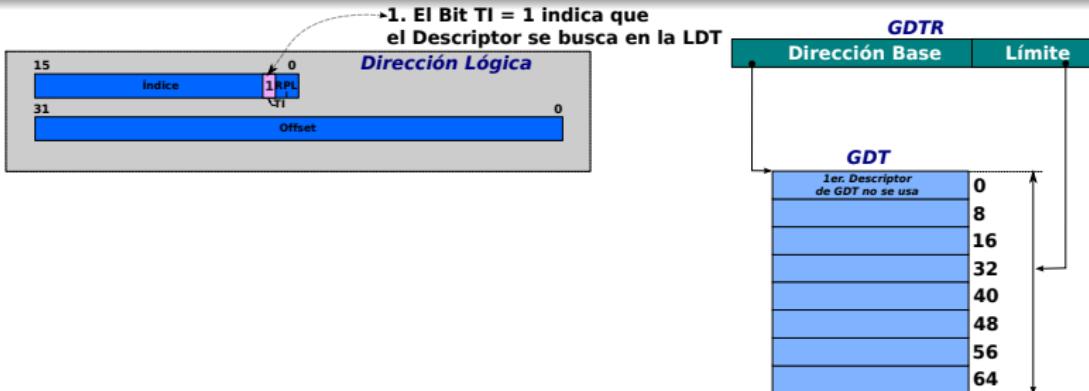
Lo que podemos observar es que partiendo de la **dirección lógica**, lo primero que trabaja el procesador es el selector y el offset recién se utiliza al final del cálculo de la **dirección lineal**. La operatoria que realiza el procesador es la siguiente:

- 1 El procesador evalúa el estado del bit 2 del selector, es decir **TI**. En este caso  $TI = 0$ , de modo que el procesador asume que buscará el descriptor en la tabla **GDT**.
- 2 El registro GDTR del procesador contiene en su campo **Dirección Base** la **dirección física** en donde comienza la **GDT**.
- 3 El valor **n** contenido por los 13 bits del campo Index del selector, referencia al  $n$ -ésimo elemento de la tabla **GDT**.
- 4 El procesador accede a la dirección de **memoria física** dada por:  $GDT.\text{Base} + 8 * \text{Index}$  y lee 8 bytes a partir de ella.
- 5 Una vez leído el descriptor, internamente reordena la **Dirección Base** y el **Límite** y agrupa los **Atributos**.
- 6 La Unidad de protección verifica que el offset contenido en el registro correspondiente de la **dirección lógica** corresponda al rango de offsets válidos del segmento de acuerdo al valor del campo **Límite**, y de los bits de **Atributos G, D/B, y ED**.
- 7 La Unidad de protección chequea que la operación a realizarse en el segmento se corresponda con los bits de **Atributos R y C**, si es de código, **W** si es de datos, que el código de acceso tenga los privilegios necesarios de acuerdo a los bits **DPL** del descriptor, que **P = 1**, entre los mas comunes.
- 8 Si todo está de manera correcta, el procesador suma el valor de offset contenido en la **dirección lógica**, con la **Dirección Base** del segmento y conforma la **dirección lineal**



8

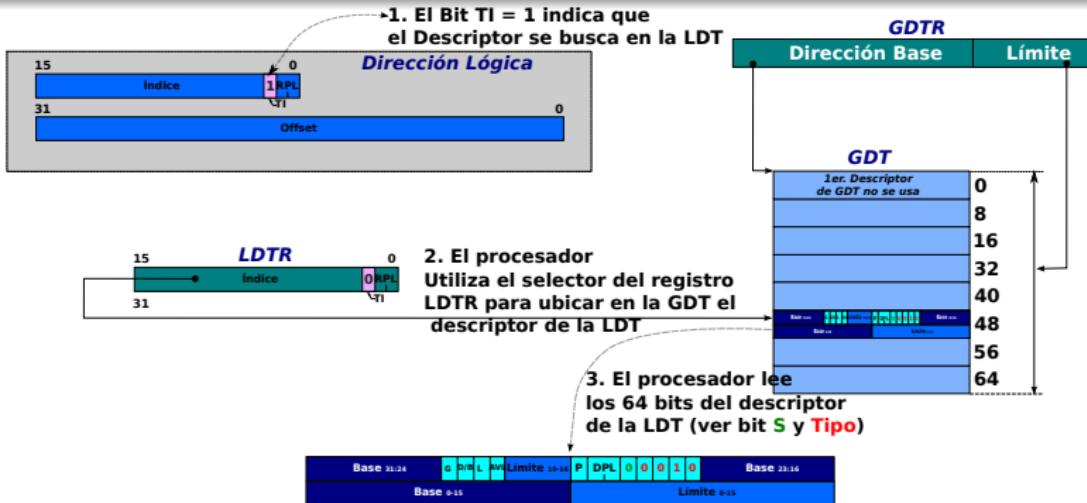
# Descriptoros de Segmento en la LDT ( $TI = 1$ )



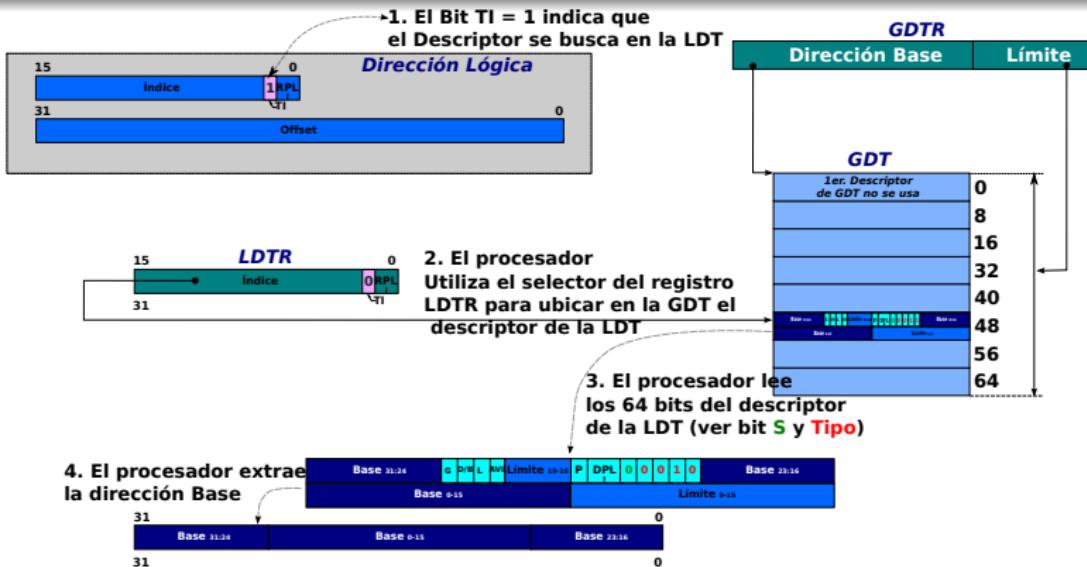
# Descriptoros de Segmento en la LDT ( $TI = 1$ )



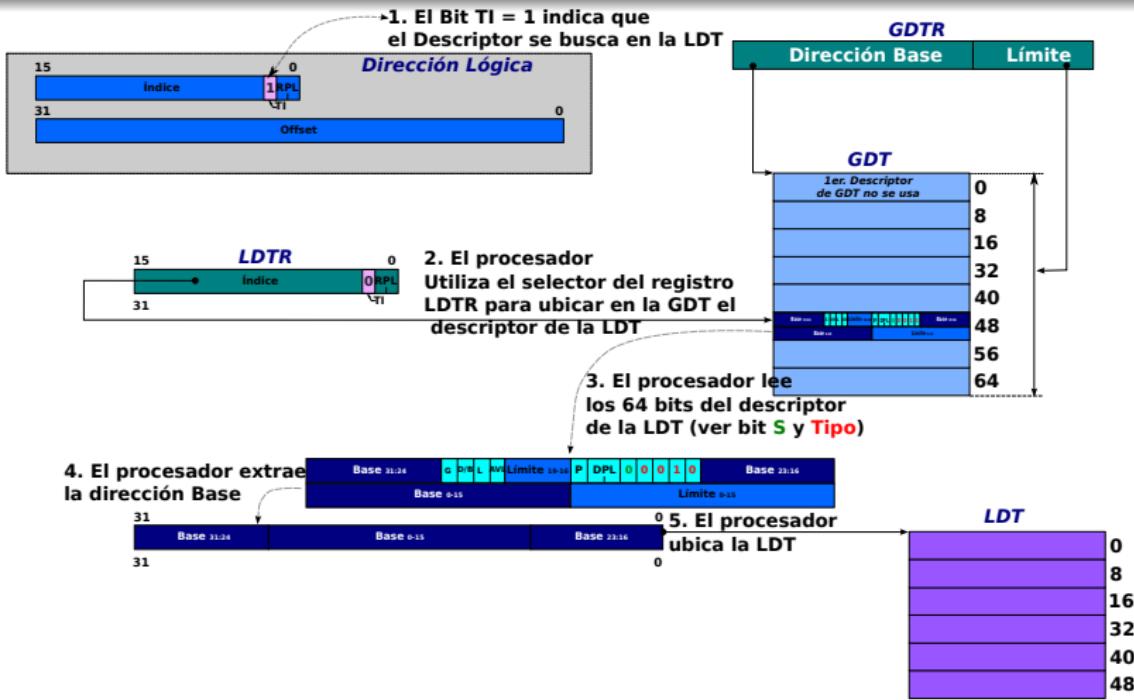
# Descriptoros de Segmento en la LDT (***TI*** = 1)



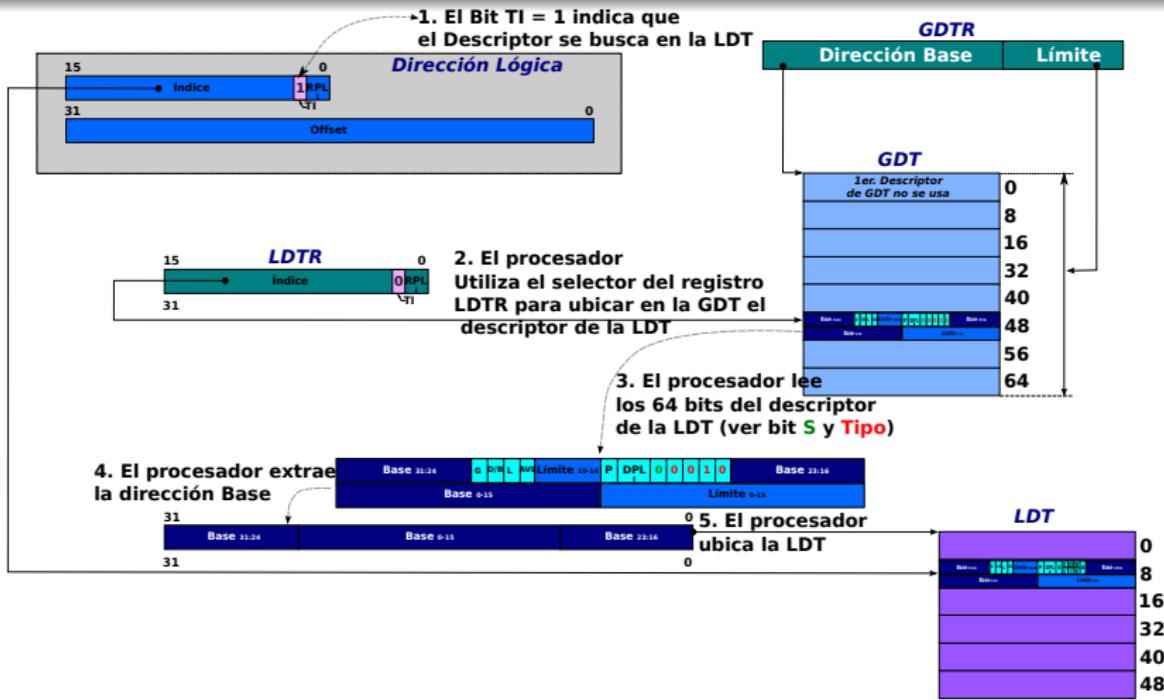
# Descriptoros de Segmento en la LDT (***TI*** = 1)



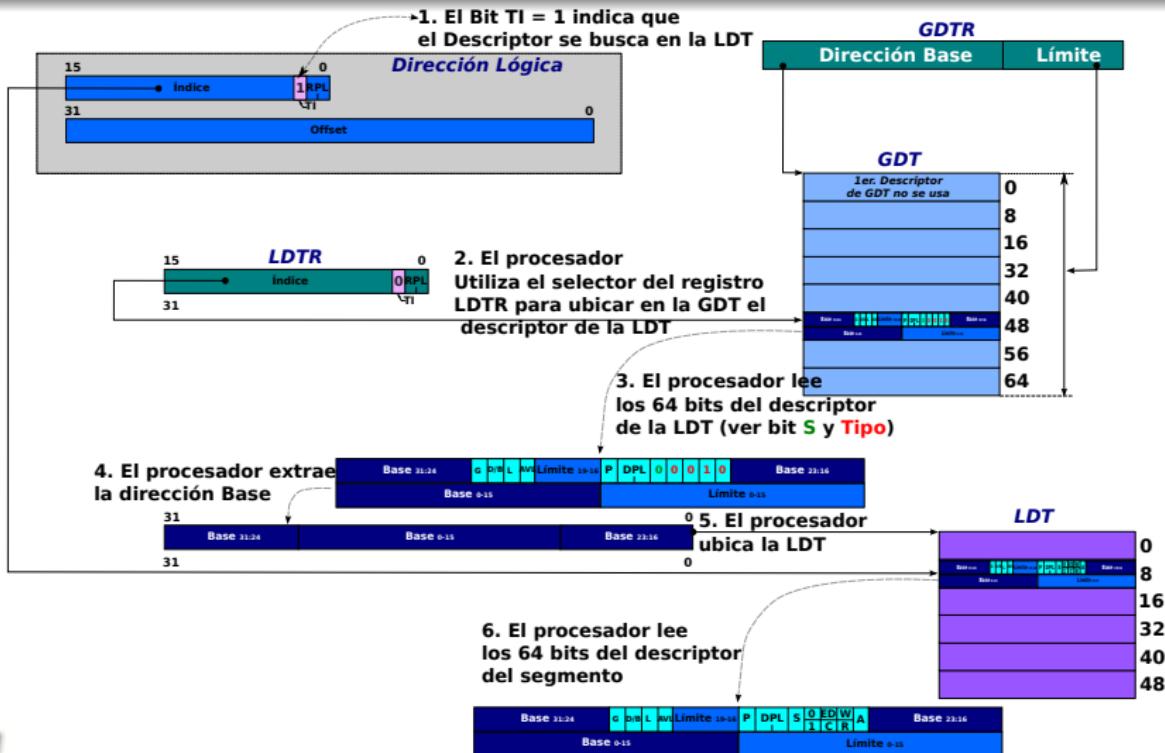
# Descriptoros de Segmento en la LDT (***TI*** = 1)



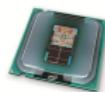
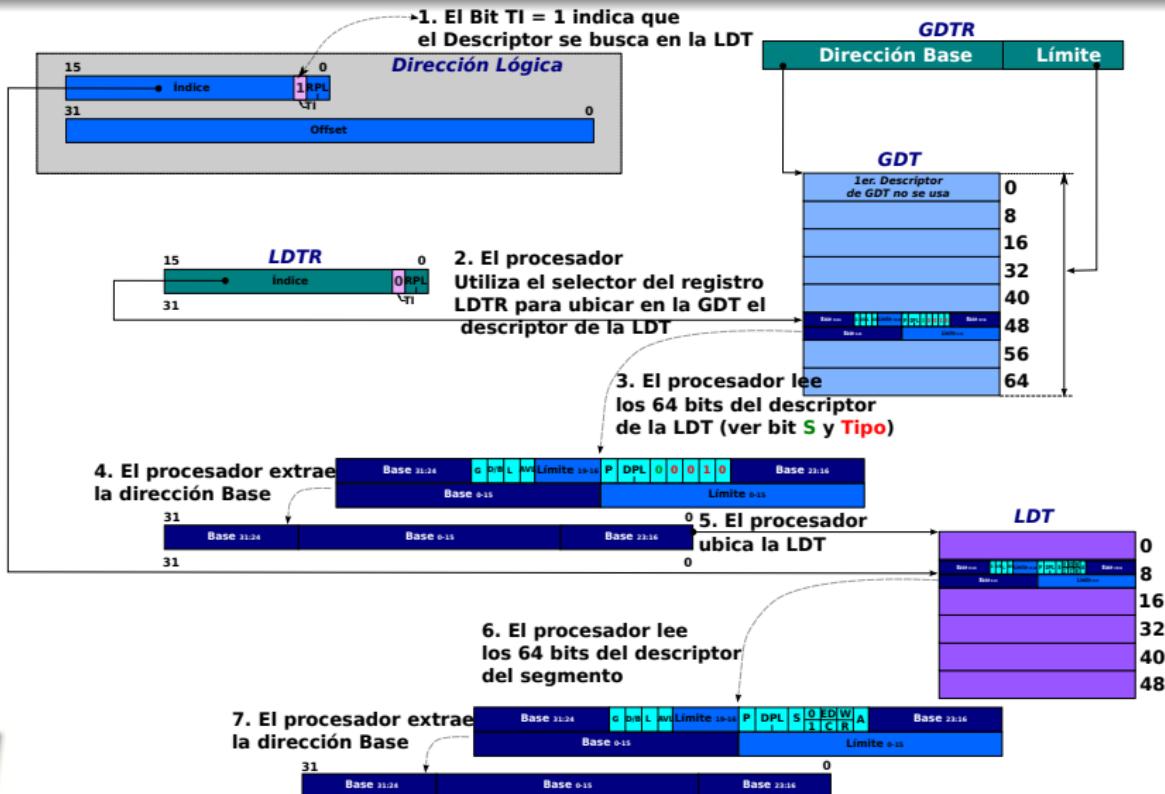
# Descriptoros de Segmento en la LDT (***TI*** = 1)



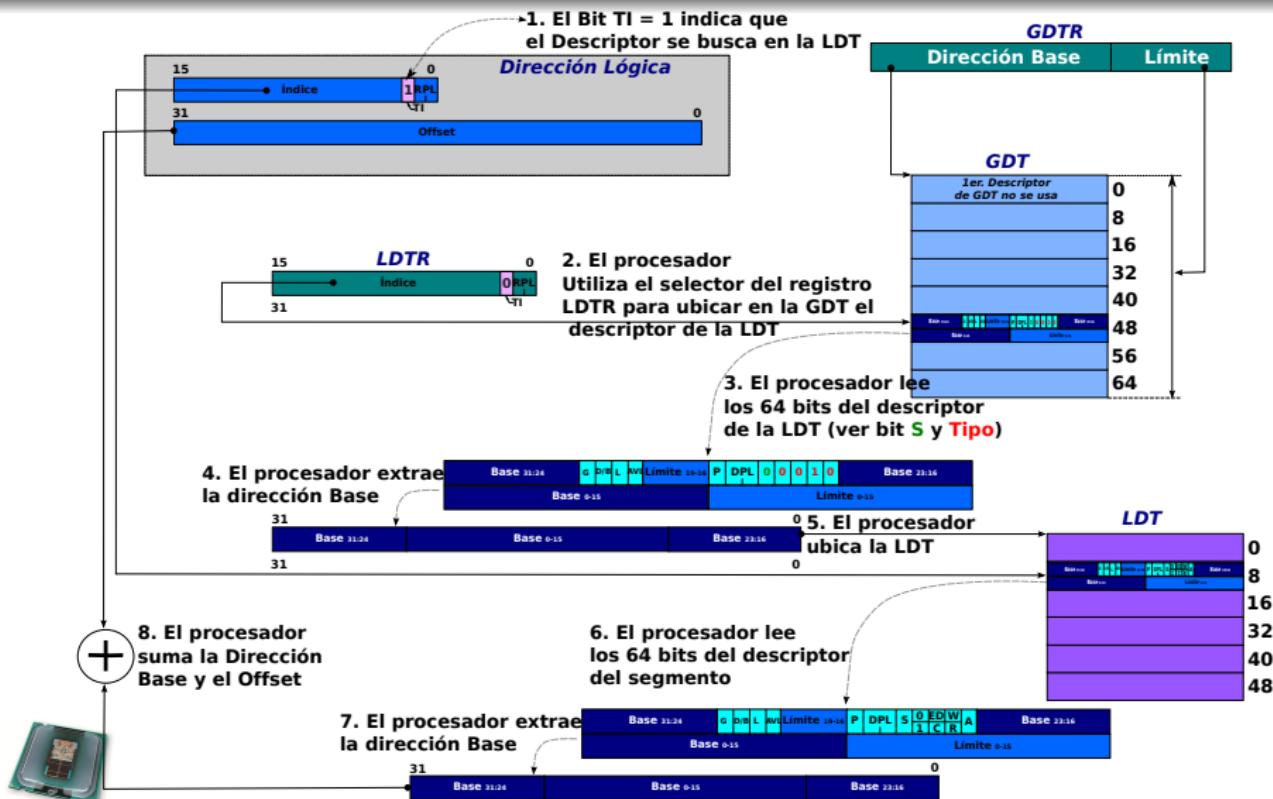
# Descriptoros de Segmento en la LDT (***TI*** = 1)



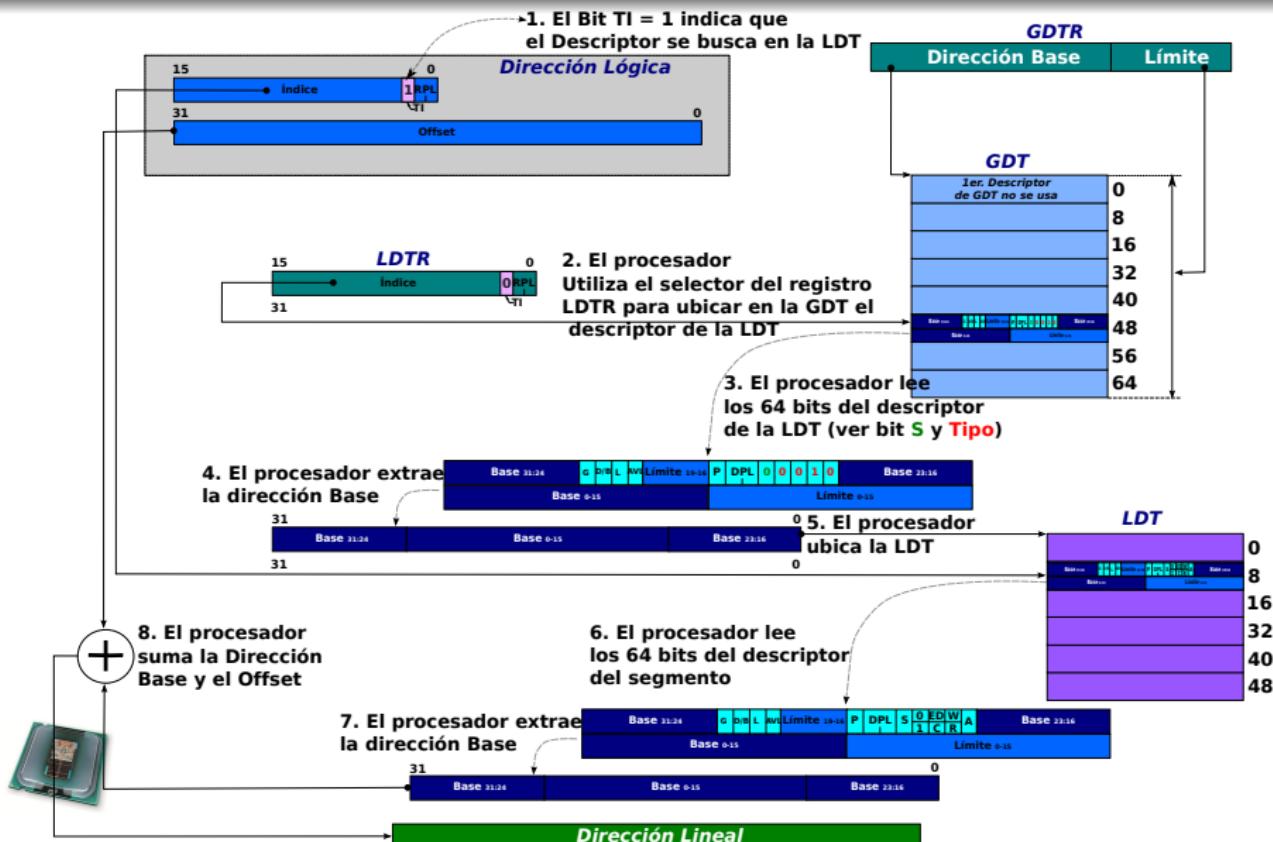
# Descriptoros de Segmento en la LDT (***TI*** = 1)



# Descriptoros de Segmento en la LDT (***TI*** = 1)



# Descriptoros de Segmento en la LDT (***TI*** = 1)



# Descriptoros de Segmento en la LDT (**TI** = 1)

La operatoria en este caso es la siguiente:

- 1 El procesador evalúa el estado del bit 2 del selector, es decir **TI**. En este caso **TI** = 1, de modo que el procesador asume que buscará el descriptor en la tabla **LDT**.
- 2 El registro LDTR del procesador contiene el selector de segmento que permitirá ubicar en la **GDT**el descriptor de sistema del segmento que contiene la **LDT**. Por lo tanto antes de trabajar con la **dirección lógica** , el procesador necesita obtener la **LDT**.
- 3 El valor **n** contenido por los 13 bits del campo Index del selector presente en el registro LDTR, referencia al n-ésimo elemento de la tabla **GDT**. En ese sitio de la GDT debe haber necesariamente un descriptor de segmento de sistema, cuyo valor en el campo Tipo sea 0010, es decir el código binario correspondiente a un descriptor de **LDT**. De otro modo el procesador generará una excepción.
- 4 El procesador accede a la dirección de **memoria física** dada por:  $GDT.\text{Base} + 8 * \text{Index}$  y lee 8 bytes a partir de ella.
- 5 Una vez leído el descriptor, internamente reordena la **Dirección Base** , comprueba los **Atributos** , en especial que el valor del bit S sea 0 y que el descriptor corresponda a un Descriptor de **LDT**(es decir Tipo = 0010).



# Descriptoros de Segmento en la LDT ( $TI = 1$ )

- ⑥ Una vez leído y validado el descriptor de segmento de la **LDT**, el procesador puede leer desde la **LDT** el descriptor del segmento de la **dirección lógica**. Para ello utiliza, ahora si, el valor **n** contenido por los 13 bits del campo Index del selector de segmento que compone dicha **dirección lógica**, que referenciará al n-ésimo elemento de la tabla **LDT**.
- ⑦ El procesador accede a la dirección de **memoria física** dada por:  $LDT.Base + 8 * Index$  y lee 8 bytes a partir de ella.
- ⑧ Una vez leído el descriptor del segmento, la Unidad de protección verifica que el offset contenido en el registro correspondiente de la **dirección lógica** corresponda al rango de offsets válidos del segmento de acuerdo al valor del campo **Límite**, y de los bits de **Atributos G, D/B, y ED**.
- ⑨ La Unidad de protección chequea que la operación a realizarse en el segmento se corresponda con los bits de **Atributos R y C**, si es de código, **W** si es de datos, que el código de acceso tenga los privilegios necesarios de acuerdo a los bits **DPL** del descriptor, que **P = 1**, entre los mas comunes.
- ⑩ Si todo está de manera correcta, el procesador suma el valor de offset contenido en la **dirección lógica**, con la **Dirección Base** del segmento y conforma la **dirección lineal**

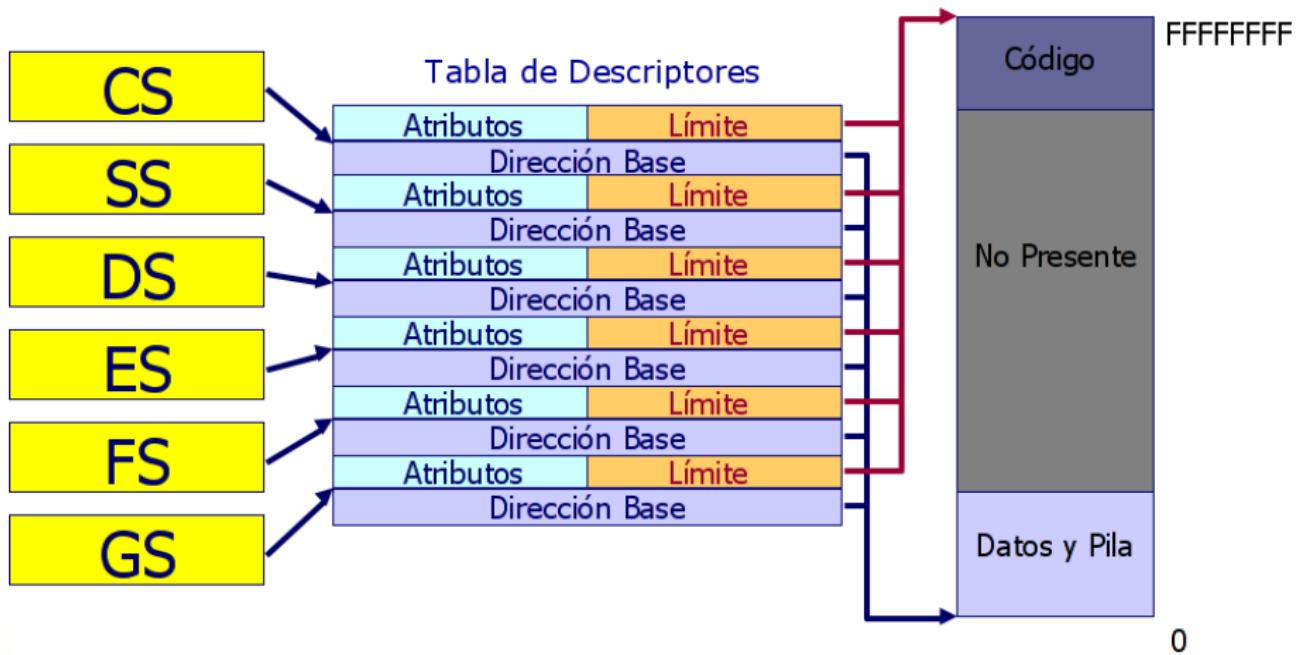


# Registros cache ocultos (hidden)

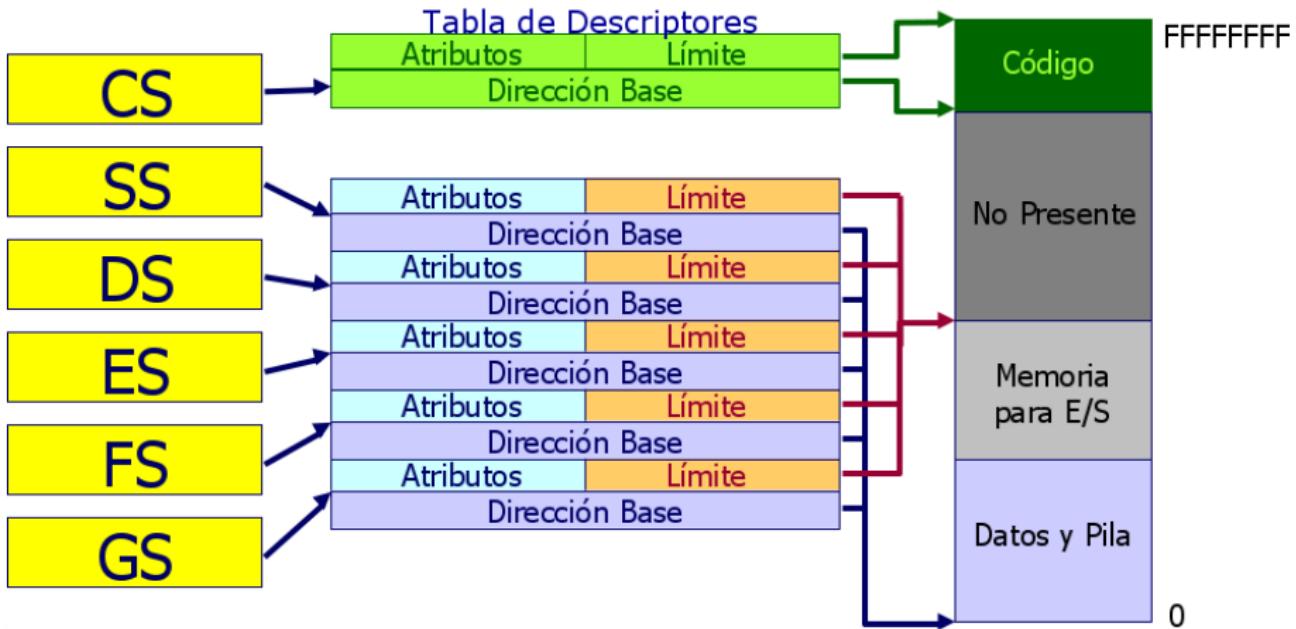
CS	Dirección Base	Límite	Atributos
SS	Dirección Base	Límite	Atributos
DS	Dirección Base	Límite	Atributos
ES	Dirección Base	Límite	Atributos
FS	Dirección Base	Límite	Atributos
GS	Dirección Base	Límite	Atributos
LDTR	Dirección Base	Límite	Atributos
TR	Dirección Base	Límite	Atributos

Cuando el procesador trabaja en modo 64 bits los tamaños de los campos del descriptor se ajustan para contener los valores correspondientes a los selectores de 64 bits.

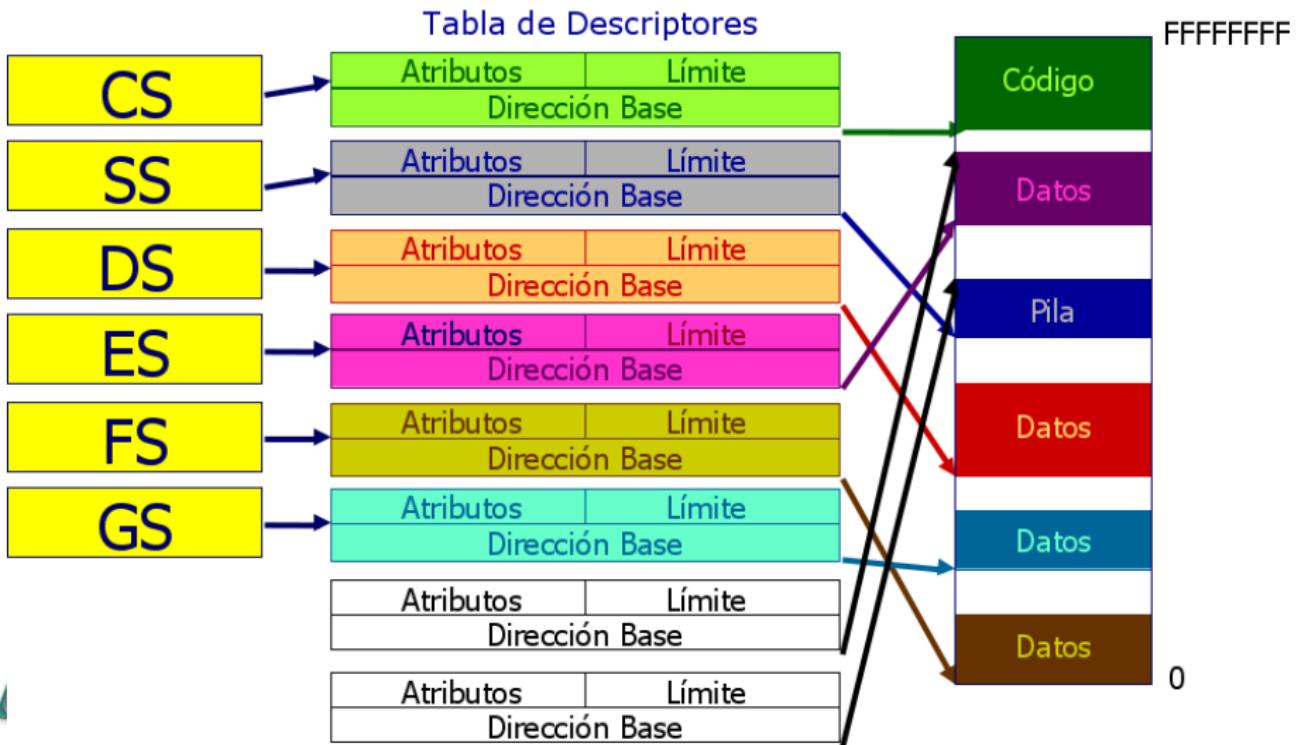
# Modelo Flat



# Modelo Flat Protegido



# Modelo Multisegmento



- 1 Administración de memoria
  - Enfoque preliminar
  - Gestión de la Memoria
- 2 Como se organiza la memoria en procesadores x86
  - Modelo de memoria en Modo Protegido
  - Modelo de memoria en Modo 64 bits
- 3 Direcciones Lógicas y Lineales
  - Traducción de direcciones Lógicas
- 4 Unidad de Segmentación
  - Selectores de segmento
  - Descriptores de segmento de 32 bits
- 5 Generación de la dirección Lineal (32 bits)
- 6 Modelos de segmentación de memoria
- 7 Segmentación en Modo IA-32e
  - Implementación práctica de segmentación en un SO
- 8 Paginación
  - Introducción
  - Unidad de Paginación - IA32
  - Paginación en IA-32 (32 bits)
  - Formatos de descriptores de página
  - Paginación PAE
  - Paginación IA-32e
  - Niveles vs. Modos de paginación
- 9 Paginación en ARMv7 Cortex-A y Cortex-R
  - Introducción
  - Memory Management Unit
- 9 Paginación en un Sistema Operativo Real: Linux



# Segmentación - -

- Si el procesador está seteado en el modo IA-32e, el submodo de trabajo depende del valor del atributo **L** del descriptor segmento de código que contiene el código actualmente en ejecución.
- Si **L** = 0 el procesador está en el sub modo Compatibilidad con lo cual, el tratamiento de los segmentos por parte del procesador es similar al del modo IA-32.
- En el caso que **L** = 1, el procesador está en el sub modo de 64 bits, y si bien mantiene la segmentación, prácticamente la deshabilita, generando un espacio lineal FLAT de 64 bits, en el que **CS**, **SS**, **DS**, y **ES**, tienen una dirección base 0, de modo que la **dirección lineal** se iguala a la efectiva u offset dentro del segmento. Los registros **FS** y **GS**, son la excepción pudiendo definir direcciones base diferentes. Esta diferencia en el tratamiento tiene por objeto facilitar algunas operaciones del sistema operativo y acceso a datos locales.



# Chequeo del límite en modo IA-32e

## Sub-modo 64 bits

- El procesador no chequea el Límite del segmento. Vale decir que en este modo los registros **SS**, **DS**, y **ES**, se ignoran prácticamente, por lo tanto, sus registros cache Hidden son ignorados.
- Cualquier referencia a ellos en una **dirección lógica** se trata como si su base fuese cero siempre. En base a ello, algunas operaciones de carga de registros de segmento resultan inválidas, como Mov Sreg, POP Sreg, LDS, LES y otras.
- Por lo demás la generación de una **dirección lineal** es similar a lo explicado en el modo 32 bits, solo que al ser la base 0, siempre coincide con el offset, y el resultado es una dirección de 64 bits que deberá estar en formato canónico, ya que de lo contrario el procesador generará una excepción #GP.

# Carga de descriptores

## Sub-modo Compatibilidad

- En el Sub Modo Compatibilidad, las instrucciones de carga de registros de segmento funcionan normalmente en cuanto al procedimiento de búsqueda del descriptor en la tabla *GDT o LDT*, su lectura por parte del procesador, y escritura de los campos de los registros Hidden del registro de segmento en cuestión acorde con los valores de los campos Base Límite y Atributos del descriptor leído. No obstante, los valores de los registros Hidden son ignorados durante la ejecución del código.
- Cuando se sobre escriben en un programa los registros **FS** y **GS**, se calcula la **dirección lineal** en base al valor de dirección base almacenado en el registro cache Hidden del registro de segmento. Puede resultar que el valor de una vuelta alrededor del la dirección tope. Lo importante es que el valor resultante esté en formato canónico.

# Carga de descriptores

## Sub-modo Compatibilidad

- Cuando se usan los prefijos FS y GS para sobre escribir el default de la instrucción no se chequea límite ni atributos.
- Las cargas normales de **FS** y **GS**. cargan un valor standard de 32 bits en el campo base del registro cache Hidden del registro y ponen el resto en 0 para mantener consistencia con implementaciones que usen menos de 64 bits.
- Los campos Base del descriptor se escriben en MSRs para mantener los 64 bits de la dirección. Se trata de **FS** y **GS**. Cualquier programa que ejecute con Privilegio '00', puede ejecutar la instrucción WRMSR para escribir la dirección base completa. Si esta dirección escrita en el MSR no está en formato canónico, el resultado es una excepción #GP.
- En sub modo compatibilidad, los registros **FS** y **GS** utilizan solo los 32 bits menos significativos del campo base que esté escrito

# Carga de descriptores

## Sub Modo 64 bits

- En Modo 64 bits se incluye una instrucción nueva SWAPGS para cargar la base completa del segmento que se selecciona con el registro **GS**.
- Respecto de las tablas de descriptores, en modo IA-32e, el registro **GDTR** se expande a 80 bits para poder almacenar una base de 64 bits para la **GDT**. Lo mismo ocurre con el registro cache Hiden del **LDTR**.
- Las tablas de descriptores están dimensionadas para almacenar  $2^{13}$  estructuras de 8 bytes de tamaño. Es decir, que cada entrada a la tabla de descriptores corresponde a 8 bytes. Muchos descriptores de sistema utilizan 16 bytes para poder incluir el campo Base de 64 bits. En tal caso ocuparán el espacio de dos entradas o descriptores de segmento.

**1 Administración de memoria**

- Enfoque preliminar
- Gestión de la Memoria

**2 Como se organiza la memoria en procesadores x86**

- Modelo de memoria en Modo Protegido
- Modelo de memoria en Modo 64 bits

**3 Direcciones Lógicas y Lineales**

- Traducción de direcciones Lógicas

**4 Unidad de Segmentación**

- Selectores de segmento
- Descriptores de segmento de 32 bits

**5 Generación de la dirección Lineal (32 bits)****6 Modelos de segmentación de memoria****● Segmentación en Modo IA-32e****● Implementación práctica de segmentación en un SO****7 Paginación**

- Introducción
- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)
- Formatos de descriptores de página
- Paginación PAE
- Paginación IA-32e
- Niveles vs. Modos de paginación

**8 Paginación en ARMv7 Cortex-A y Cortex-R**

- Introducción
- Memory Management Unit

**9 Paginación en un Sistema Operativo Real: Linux**

# Lecturas indispensables

- Al tener disponibles los fuentes del sistema operativo Linux, existe abundante información de sus detalles de implementación.
- Understanding the Linux Kernel, de Daniel Bovet y Marco Cesati, Ed. O'Reilly (¿cuando no?), cuenta con muy interesantes detalles de como se utilizan los recursos de un procesador IA-32 para implementar lo que llamaríamos el kernel de bajo nivel del Sistema Operativo.
- Secciones de código que trabajan directo con los registros del procesador y detalles del hardware.
- Tener en cuenta que la última edición disponible apareció en ocasión del lanzamiento del kernel 2.6. Este kernel ha tenido evoluciones hasta el sub-release 2.6.31, y actualmente está disponible la versión de kernel 3.7. Por lo tanto es necesario revisar si no hubo actualizaciones. Afortunadamente Linux no tiene misterios y la información es pública y accesible, esto lo hace atractivo como caso de estudio.



# Hurgando en los fuentes

- A partir de la versión de kernel 2.2, (hace muchos años ya) Linux comenzó a soportar SMP (Symmetric Multi Processing), es decir la capacidad de controlar sistemas de hardware con mas de un procesador, todos iguales (por eso Symmetric).
- Cuando se lanza la versión 2.4 del kernel, Linux mejora su eficiencia en el manejo SMP manteniendo una **GDT** por cada procesador presente en el sistema. En un array denominado **cpu\_gdt\_table** guarda las estructuras de las **GDT**, correspondiendo cada elemento del arreglo a una CPU.
- El código que se emplea se muestra a continuación. En la primer línea de dicho listado, que corresponde al archivo /source/linux/include/asm-i386/desc.h de los fuentes del sistema, se declara un arreglo de GDT\_ENTRIES descriptores, en donde GDT\_ENTRIES ha sido inicializada con la cantidad de descriptores totales a almacenar en la **GDT** menos 1, ya que el primer descriptor lleva el índice 0. Es decir, que allí se define un arreglo de descriptores que arma una **GDT**.



# Hurgando en los fuentes

Hasta el momento Linux usa **GDT** de 32 entradas, definiendo en la línea 112 del archivo /source/linux/include/asm-i386/segment.h el valor a GDT\_ENTRIES en 32.

```
1 extern struct desc_struct cpu_gdt_table[GDT_ENTRIES];  
2 DECLARE_PER_CPU (struct desc_struct , cpu_gdt_table[GDT_ENTRIES  
]);
```

Donde

```
1 #define GDT_ENTRIES 32
```

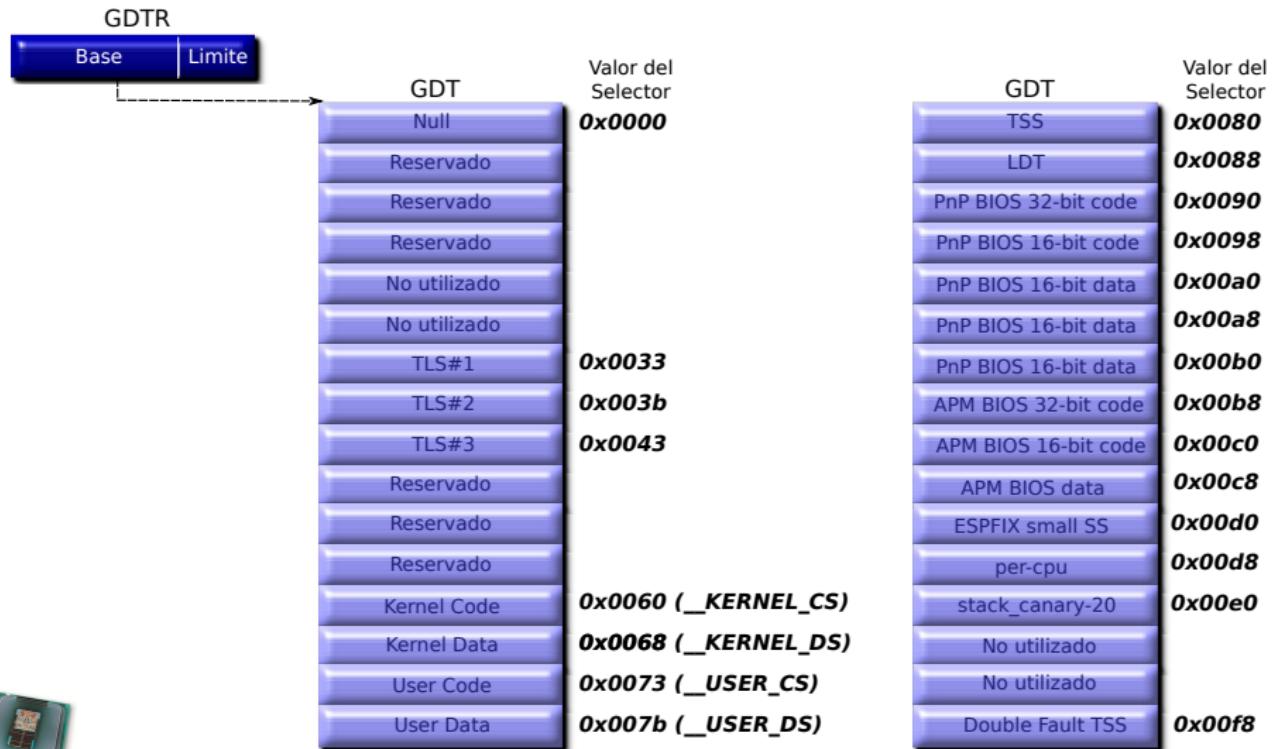
La estructura **desc\_struct** señalada como externa se define en el archivo fuente /source/linux/include/asm-i386/processor.h

```
1 struct desc_struct {  
2     unsigned long a,b;  
3 };
```

En el archivo /source/linux/include/asm-i386/percpu.h se define.

```
1 #define DECLARE_PER_CPU(type , name) extern __typeof__(type)  
per_cpu_##name
```

# GDT en Linux



# Modelo de segmentación en Linux

- Los selectores de segmento 0x0060, y 0x0068, definidos por las macros \_\_KERNEL\_CS, y \_\_KERNEL\_DS, corresponden a los descriptores de código y datos respectivamente del kernel.
- Por su parte los selectores 0x0073 y 0x007b definidos por las macros \_\_USER\_CS, y \_\_USER\_DS, corresponden a los descriptores de código y datos respectivamente de modo usuario.
- Además estos descriptores tiene los siguientes valores dentro de la tabla siguiente.

Selector	Base	G	Límite	S	Tipo	DPL	D/B
__USER_CS	0x00000000	1	0xfffff	1	1010	11	1
__USER_DS	0x00000000	1	0xfffff	1	0010	11	1
__KERNEL_CS	0x00000000	1	0xfffff	1	1010	00	1
__KERNEL_DS	0x00000000	1	0xfffff	1	0010	00	1

**Conclusión:** Linux utiliza un modelo de segmentación FLAT Básico.



# Descriptoros de Sistema

## 1 TSS

- Un descriptor de **TSS** único por cada CPU. (ampliaremos su significado al abordar el tema Tareas).
- Linux mantiene un array denominado **init\_tss**
- Cada descriptor de **TSS** contendrá una dirección Base que apunta al la dirección de inicio del TSS de esa CPU dentro de este array.

## 2 Un Descriptor de **LDT** default común para todas las tareas por cada CPU. En principio no se utilizan segmentos locales.

- Este array se define en el archivo

`linux/include/asm-i386/desc.h` con la línea que se muestra en el listado siguiente.

```
1 extern struct desc_struct default_Idt [];
```

- Por otra parte, en el archivo `/source/linux/arch/i386/kernel/traps.c` se inicializa una **LDT** por default para cada CPU que se incluirá al armar la estructura de tablas. Se muestra en el listado siguiente. Como vemos se genera un arreglo de 5 descriptoros nulos.

```
1 struct desc_struct default_Idt [] = { { 0, 0 }, { 0, 0 }
              , { 0, 0 } , { 0, 0 } , { 0, 0 } , { 0, 0 } };
```



**1 Administración de memoria**

- Enfoque preliminar
- Gestión de la Memoria

**2 Como se organiza la memoria en procesadores x86**

- Modelo de memoria en Modo Protegido
- Modelo de memoria en Modo 64 bits

**3 Direcciones Lógicas y Lineales**

- Traducción de direcciones Lógicas

**4 Unidad de Segmentación**

- Selectores de segmento
- Descriptores de segmento de 32 bits

**5 Generación de la dirección Lineal (32 bits)****6 Modelos de segmentación de memoria**

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

**7 Paginación****● Introducción**

- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)
- Formatos de descriptores de página
- Paginación PAE
- Paginación IA-32e
- Niveles vs. Modos de paginación

**8 Paginación en ARMv7 Cortex-A y Cortex-R**

- Introducción
- Memory Management Unit

**9 Paginación en un Sistema Operativo Real: Linux**

# Paginación de la Memoria

- Segmentación:

- Provee un entorno flexible en la programación de aplicaciones.
- Para la administración de la memoria por parte del sistema operativo, la variabilidad del tamaño de los segmentos introduce complejidad en los algoritmos de un sistema de memoria virtual.



# Paginación de la Memoria

- Paginación

- Mas rígido para aplicar en la programación de aplicaciones.
- Trabajar con bloques del mismo tamaño, simplifica el desarrollo del algoritmo de memoria virtual.



# Paginación de la Memoria

- Esto ha hecho que tradicionalmente los sistemas operativos hayan diseñado su sistema de memoria virtual mediante la administración de bloques de memoria de tamaño fijo.
- De hecho, UNIX por citar al decano de los Sistemas Operativos, desde su concepción implementó la administración de la memoria utilizando bloques de tamaño uniforme.



**1** Administración de memoria

- Enfoque preliminar
- Gestión de la Memoria

**2** Como se organiza la memoria en procesadores x86

- Modelo de memoria en Modo Protegido
- Modelo de memoria en Modo 64 bits

**3** Direcciones Lógicas y Lineales

- Traducción de direcciones Lógicas

**4** Unidad de Segmentación

- Selectores de segmento
- Descriptores de segmento de 32 bits

**5** Generación de la dirección Lineal (32 bits)**6** Modelos de segmentación de memoria

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

**7** Paginación

- Introducción
- **Unidad de Paginación - IA32**
- Paginación en IA-32 (32 bits)
- Formatos de descriptores de página
- Paginación PAE
- Paginación IA-32e
- Niveles vs. Modos de paginación

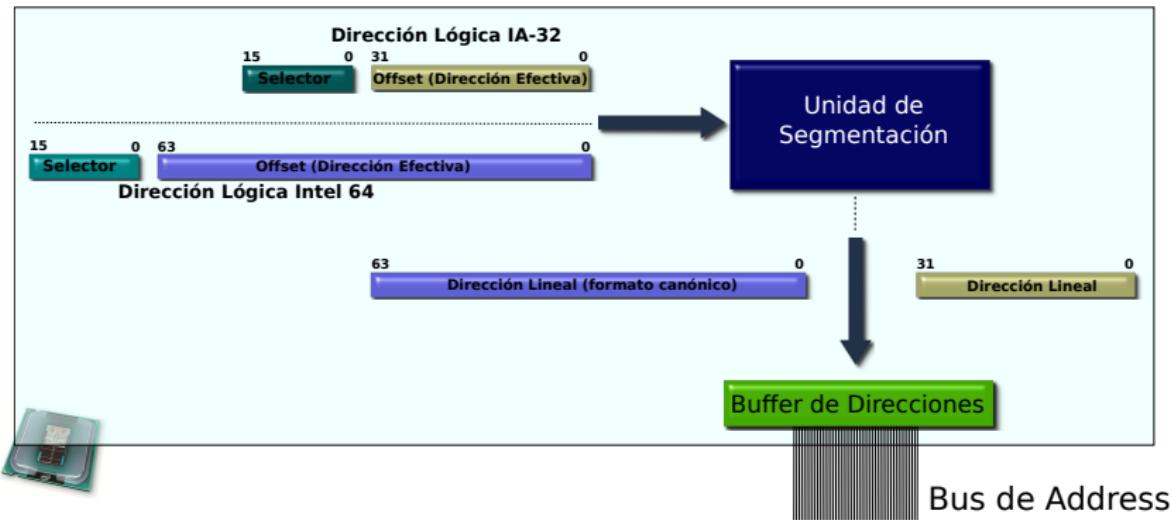
**8** Paginación en ARMv7 Cortex-A y Cortex-R

- Introducción
- Memory Management Unit

**9** Paginación en un Sistema Operativo Real: Linux

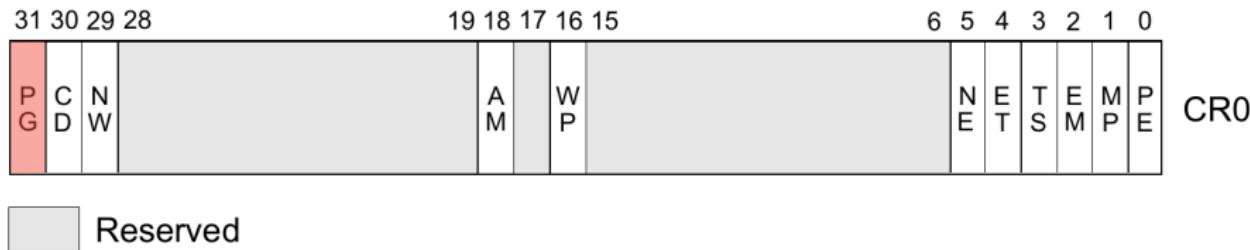
# Diagrama de generación de la dirección física

- Un segmento es finalmente un espacio lineal de direcciones, razón por la cual se denomina a este número de 32 o 64 bit obtenido por la Unidad de Segmentación, **dirección lineal**
- De no mediar otra etapa, de hardware, este número sale por el bus de Address convertido en **dirección física**



# Habilitación de la Paginación

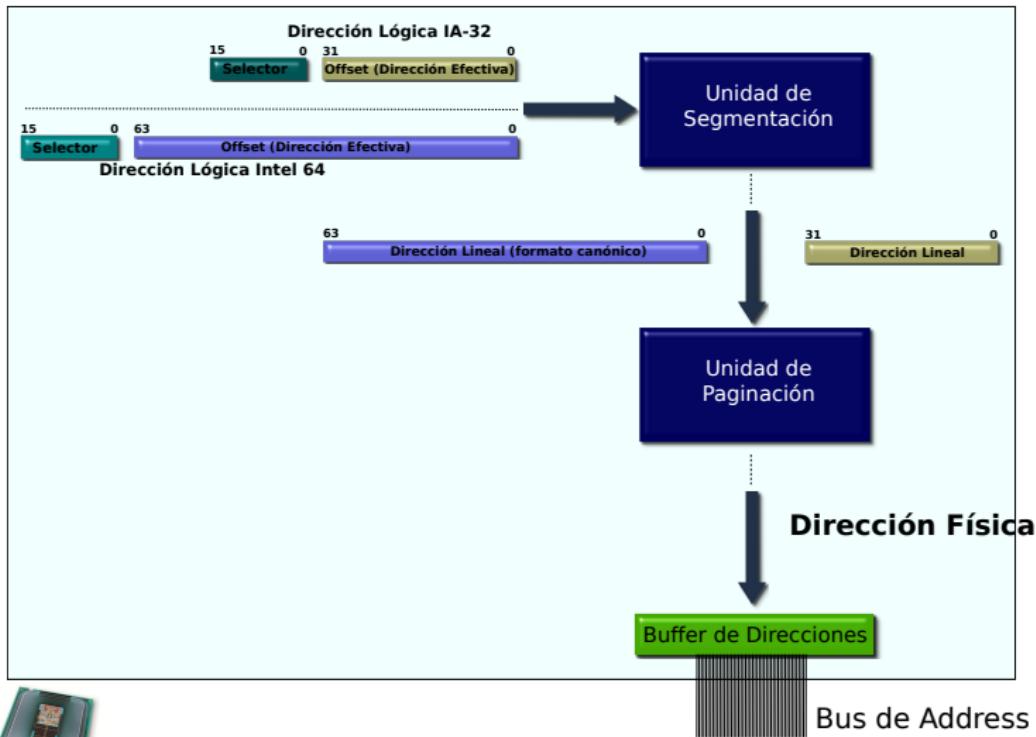
La Unidad de Paginación debe habilitarse seteando el bit **CR0.PG**



**Importante:** El procesador debe estar previamente en Modo Protegido, de otro modo #GP.



# Diagrama de generación de la dirección física



# Unidad de Paginación IA-32

La Unidad de Paginación, permitió a los procesadores IA-32 :

- Fraccionar el espacio lineal de un segmento en páginas de menor tamaño.
- Así el Sistema Operativo tiene en RAM únicamente unas pocas páginas de cada segmento
- El resto en la Memoria Virtual para ser intercambiadas cuando se las necesite. No requiere el segmento completo el RAM.
- Así el Sistema Operativo puede alojar en memoria mayor cantidad de procesos, ya que cada uno requiere menos memoria para iniciar su ejecución.



# Unidad de Paginación IA-32

La Unidad de Paginación, permitió a los procesadores IA-32 :

- El software por lo general se construye de una serie de estructuras de iteración.
- O sea que una página de memoria de código puede ser ejecutada durante muchos ciclos de clock antes de requerirse otra.
- Por lo tanto la frecuencia con que cada proceso bien programado requeriría bajar desde la Memoria Virtual otra página a la memoria Física, será bastante moderada.
- En la práctica, disponer de paginación permitió ejecutar por primera vez un Sistema Operativo UNIX, en un procesador Intel.



# Modos de paginación

**32 Bits** Es el modo original de paginación del 80386 (1984): páginas de 4 Kbytes. Con el lanzamiento del procesador Pentium Pro (1995) un modo de extensión de memoria física y tamaño de página denominado PSE (Page Size Extension).



# Modos de paginación

**PAE** Introducido junto con PSE en el Pentium Pro, es el método que finalmente adoptaron los Sistemas Operativos como Linux para generar kernels de 32 bits capaces de acceder a direcciones de memoria mas allá de los 4 Gbytes. Por este motivo desde entonces hasta el presente se ha “ganado” el derecho a que se lo considere un modo en si mismo.



# Modos de paginación

- IA-32e** Basado en el PAE, es el modo de paginación que se utiliza cuando el procesador se setea en modo IA-32e, es decir, 64 bits puro.



**1 Administración de memoria**

- Enfoque preliminar
- Gestión de la Memoria

**2 Como se organiza la memoria en procesadores x86**

- Modelo de memoria en Modo Protegido
- Modelo de memoria en Modo 64 bits

**3 Direcciones Lógicas y Lineales**

- Traducción de direcciones Lógicas

**4 Unidad de Segmentación**

- Selectores de segmento
- Descriptores de segmento de 32 bits

**5 Generación de la dirección Lineal (32 bits)****6 Modelos de segmentación de memoria**

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

**7 Paginación**

- Introducción
- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)**
- Formatos de descriptores de página
- Paginación PAE
- Paginación IA-32e
- Niveles vs. Modos de paginación

**8 Paginación en ARMv7 Cortex-A y Cortex-R**

- Introducción
- Memory Management Unit

**9 Paginación en un Sistema Operativo Real: Linux**

# Paginación IA-32: Páginas de 4 Kbytes

- El procesador 80386, adoptó un tamaño de página de 4 Kbytes.
- Este tamaño es entonces el tamaño estándar que por default usa cualquier procesador subsiguiente que active la paginación (compatibilidad).
- A partir del Pentium Pro se han incluido otros tamaños de página, pero si se desea utilizar páginas de diferente tamaño que 4 Kbytes, siempre debe ser explícitamente seleccionado el otro tamaño.
- El espacio lineal de 4 Gbytes, se divide en páginas de 4 Kbytes de manera completa (es decir  $2^{20}$  páginas).



# Estructuras necesarias

- Al igual que cuando hubo de tratar con los segmentos, el procesador necesitará similar información para tratar a las páginas.

**Dirección base** Necesitamos saber en donde comienza cada página.

**Límite** Necesitamos saber donde finaliza cada página.

**Atributos de acceso** Inevitablemente se necesitarán algunos bits para determinar permisos y derechos de acceso.



# Estructuras necesarias

- Aunque hay algunas simplificaciones, a saber:

## Dirección base :

- Cada página comienza en la dirección de memoria siguiente a la del último byte de la página anterior.
- Es decir: inician a partir de direcciones de memoria alineadas a su tamaño.
- Tamaño de la página =  $2^n$ . En páginas de 4 Kbytes ( $2^{12}$  bytes) los 12 bits menos significativos de su dirección base valen siempre 0.
- Dirección Base o **Page Frame** (marco de página) es el conjunto de bits mas significativos de la dirección de la página que necesitamos para especificar su dirección base.



# Estructuras necesarias

- Aunque hay algunas simplificaciones, a saber:

**Límite** No hace falta especificarlo, ya que las páginas tienen tamaño fijo.

**Atributos de acceso** Inevitablemente se necesitarán algunos bits para determinar permisos y derechos de acceso.

- **Conclusión:** Con 20 bits para la dirección base de la página mas 12 bits para los atributos podemos conformar un descriptor de páginas de 32 bits.



# ¿Cuantas páginas cubren el espacio lineal?

- Si las páginas son de 4 Kbytes ( $2^{12}$  bytes) y el espacio lineal máximo a paginar es de 4 Gbytes ( $2^{32}$  bytes), páginas que necesitamos para cubrirlo de manera completa es:

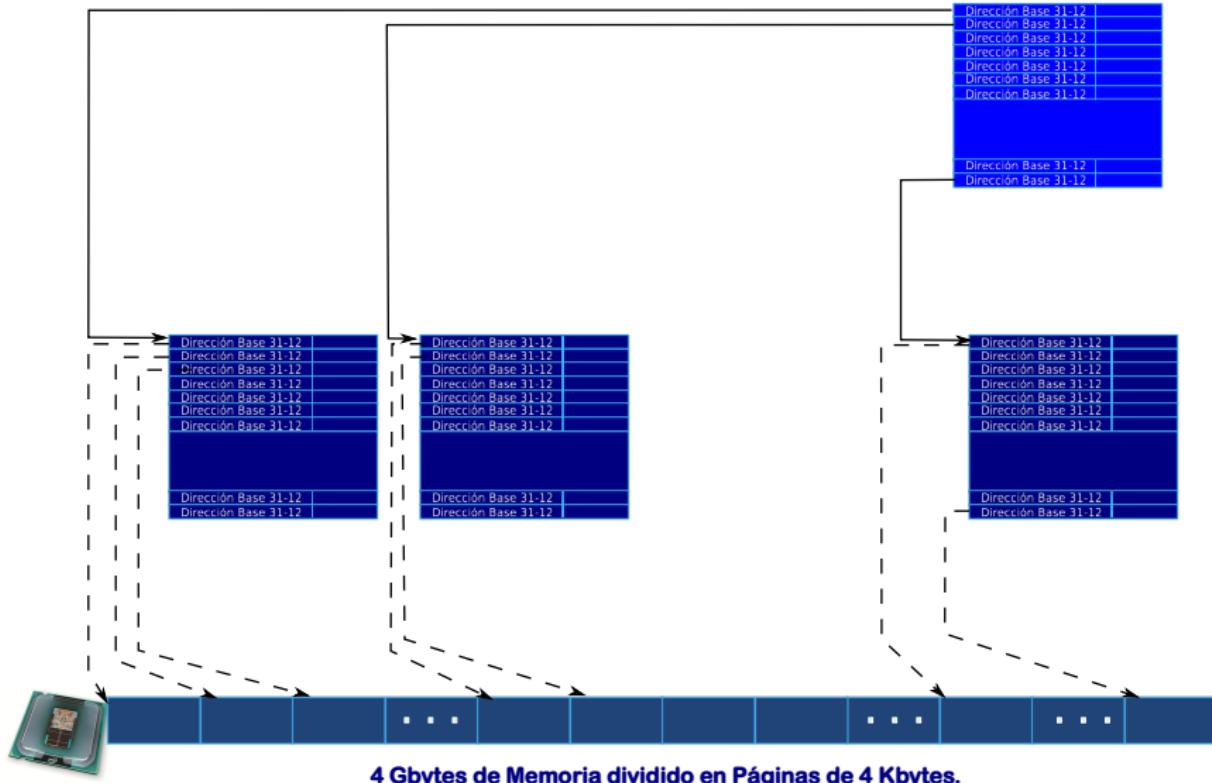
$$\frac{2^{32}}{2^{12}} = 2^{20} \quad (1)$$

- Esta situación deriva en una tabla de descriptores de página gigantesca: En este caso,  $2^{20}$  descriptores de 4 bytes, nos llevan a una tabla que ocupa 4 MBytes de memoria física.
- Por ello conviene pasar a estructuras tablas de descriptores de paginación por niveles.

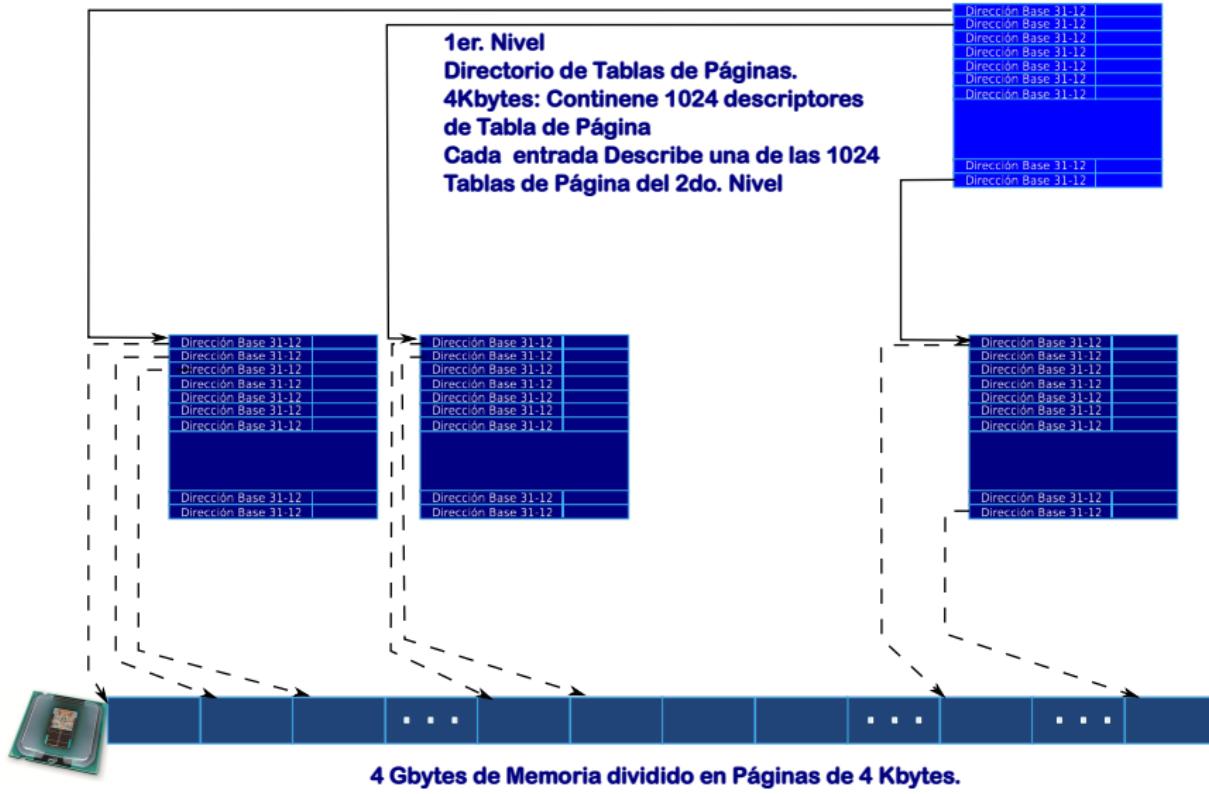


¿Como por niveles?... Veamos.

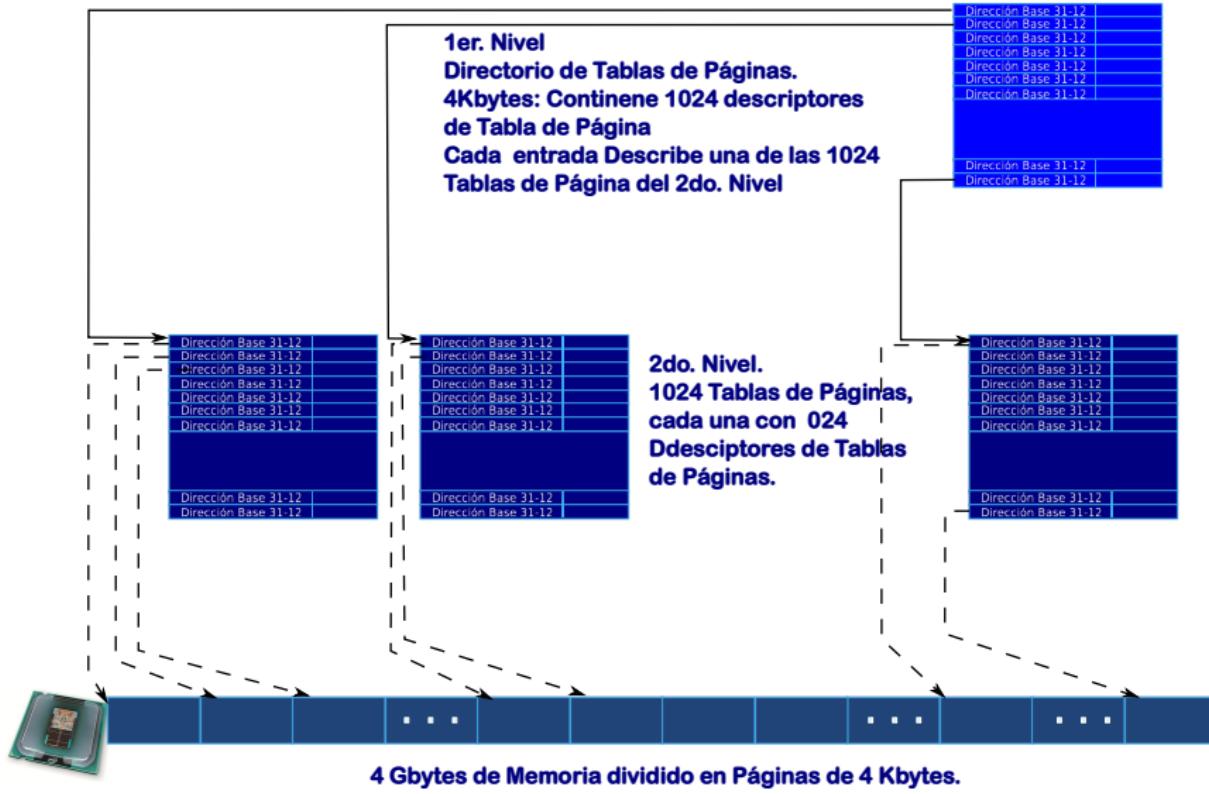
# Niveles de Paginación



# Niveles de Paginación

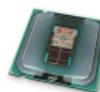


# Niveles de Paginación



# Paginas y tareas...

- La implementación en IA-32 de la paginación se ha pensado como un sistema de administración de memoria por tarea, de modo que cada tarea tiene su propia estructura de páginas.
- Esta característica robustece la seguridad del Sistema Operativo en la administración de memoria.
- Por esta razón una tabla de 4 Mbytes por cada tarea para gestionar la memoria es un contrasentido en términos de eficiencia.
- Se puede diseñar un sistema con una única tabla de páginas común a todas las tareas, pero tal enfoque da por tierra con la robustez en la de administración de memoria señalada anteriormente.



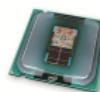
# Páginas y tareas...

- El método permite iniciar la tarea con solo dos tablas de Paginación (dos tablas = dos páginas de 4Kbytes).
  - ① Una página de 4Kbytes para el Directorio de Tablas de Página (de aquí en mas **DTP**). Estructura indispensable pues es la raíz de la jerarquía de datos. En principio contendrá tan solo un descriptor válido.
  - ② Una página de 4Kbytes para una Tabla de Páginas (de aquí en mas **PT**) apuntada por la única entrada válida del Directorio, que puede almacenar hasta 1024 descriptores de páginas válidos de 4 Kbytes c/u.



# Páginas y tareas...

- Las 1024 entradas contenidas en la **PT** describen sendas páginas de memoria que a su vez contendrán el código y los datos de la tarea.
- De este modo se puede iniciar un proceso con solo dos tablas de 4 Kbytes para administrar hasta 1024 páginas de 4 Kbytes, es decir 4 Mbytes para acomodar su código y datos.
- Esta cantidad es mas que suficiente para iniciar un proceso. ¿no?
- Por supuesto que cada proceso puede utilizar menos de 4 Mbytes de memoria al inicio (de hecho es lo habitual). Lo anterior es solo a efectos de cuantificar la cantidad de memoria que podemos asignarle consumiendo para su gestión solo 8 Kbytes.



# Administración de memoria - Guidelines

## Memoria dinámicamente alojable por proceso

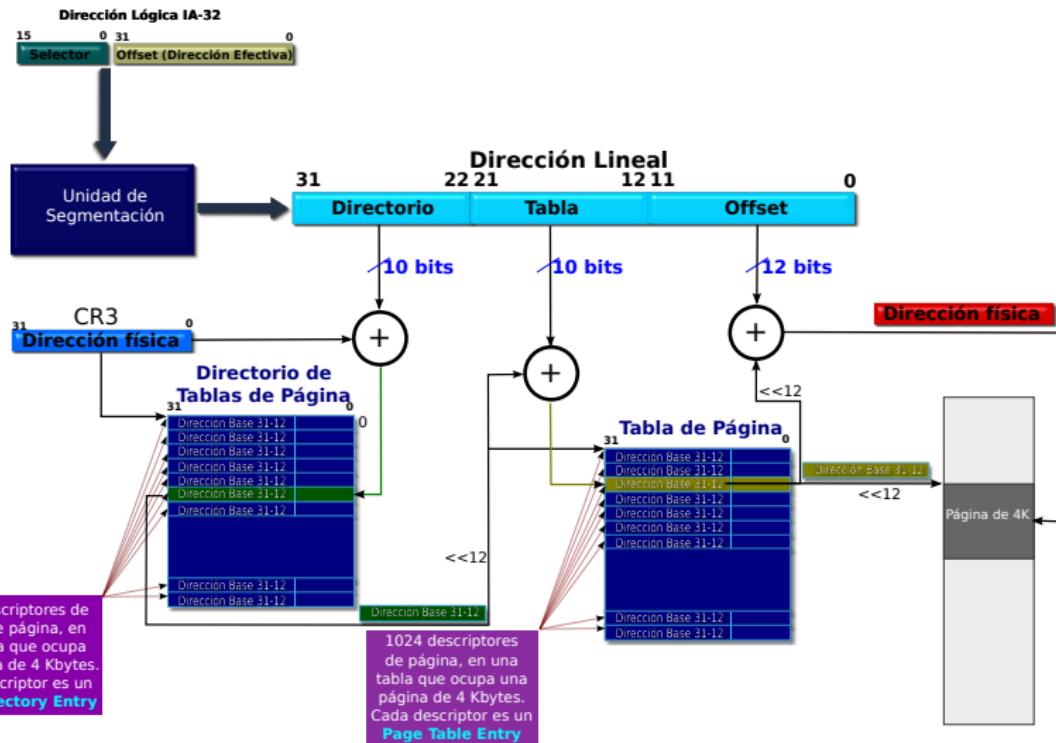
- Lo habitual es que el Sistema Operativo habilite a cada proceso unas pocas páginas para código y datos.
- Conforme el proceso requiera memoria, se irán agregando en la tabla de páginas del segundo nivel de la estructura los descriptores necesarios.
- Este procedimiento permite asignar al proceso hasta 4 Mbytes de memoria.
- Llegado a ese límite, si solicita mas memoria, se genera un segundo descriptor en el **DPT**, que permitirá habilitar otros 4 Kbytes de memoria para colocar allí hasta 1024 nuevos descriptores de Página, es decir otros 4 Mbytes máximo.

# Traducción con Páginas de 4 Kbytes en 32 bits

- Es el modo original de paginación del procesador 80386.
- El procesador necesita conocer para cada tarea, la dirección física en donde se inicia la estructura de Descriptores de Páginas.
- En estos procesador el Registro de Control **CR3** contiene esta dirección (*dirección física*).
- En el próximo slide se muestra el proceso que describiremos a continuación.
- El procesador toma la **dirección lineal** y la divide en tres campos de bits que serán utilizados respectivamente como:
  - Índice en el **DTP**, para determinar la dirección de inicio y derechos de acceso de la página que contiene la **PT** uno de cuyos descriptores corresponde a la página que se está buscando acceder en memoria física.
  - Índice en la **PT** que permitiré encontrar el descriptor de la página de memoria física que se está direccionando.
  - Desplazamiento relativo al comienzo de la página en la que se encuentra la variable o el código que se está direccionando.



# Modo 32 bits: Traducción con Páginas de 4 Kbytes



# Modo 32 bits: Traducción con Páginas de 4 Kbytes

- Como el procesador trabaja con Páginas de 4 Kbytes, las tablas se acomodarán en bloques del mismo tamaño.
- Al ser cada descriptor de página de 32 bits cada tabla podrá de este modo almacenar 1024 descriptores.
- Así tendremos que para ingresar a cada **PT** el procesador necesitará 10 bits ( $2^{10} = 1024$ ).
- Los 10 bits mas significativos de la **dirección lineal** se usan como índice en el **DPT**.
- El descriptor seleccionado (denominado **PDE**, por Page Directory Entry), contiene los 20 bits mas significativos de la dirección física de la página que contiene la **PT**.



# Modo 32 bits: Traducción con Páginas de 4 Kbytes

- Esta Tabla es la que contendrá finalmente el descriptor de la página de memoria direccionada en la MMU del procesador.
- Una vez leída la **PDE** y extraída la dirección física donde comienza la **PT**, los siguientes 10 bits de la dirección lineal se utilizan como índice en ésta para acceder al descriptor de la página direccionada.
- Esta entrada se denomina **PTE** por Page Table Entry. En el descriptor estarán los 20 bits mas significativos de la dirección física de memoria en la que comienza la página direccionada.
- Finalmente, obtenida la dirección base de la página, queda sumarle los 12 bits menos significativos de la dirección lineal se obtiene la dirección física de memoria direccionada por el procesador.



# Primeras conclusiones

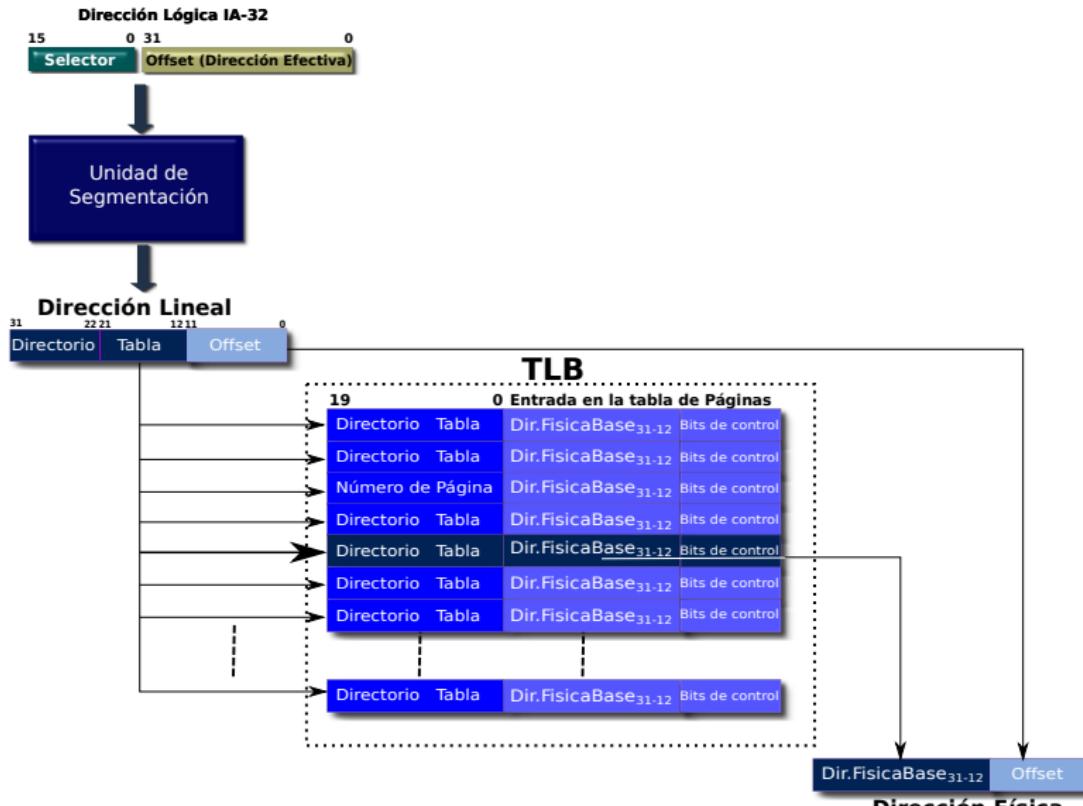
1

Del análisis de funcionamiento del mecanismo de traducción de **dirección lineal** a **dirección física** surge que no es necesario que las páginas de código estén contiguas. Si una instrucción queda al final de una página, al realizarse el próximo ciclo de fetch, el sistema de Paginación generará un par de entradas **PDE** - **PTE** diferentes de la instrucción anterior de modo que el programa ejecutará de manera transparente a la ubicación del código en memoria.

2

Por cada opcode fetch, memory read, o memory write, es necesario acceder a memoria dos veces para leer el **PDE** y el **PTE** y luego hacer sumas y demás. Al igual que en el caso de la segmentación en donde el procesador posee un cache asociado a cada registro de segmento para leer una sola vez el descriptor, en la Unidad de Paginación existe un cache de traducciones: el Translation Lookaside Buffer (o TLB)

# Translation Lookaside Buffer (TLB)



# Translation Lookaside Buffer (TLB)

- Se almacenan solo las partes de interés de las direcciones lineal y física.
- Mas específicamente, los bits de la **dirección lineal** que se utilizan para acceder al **DTP**, y a la **PT**, y los bits de la **dirección física** contenidos en el descriptor de la página direccionada, es decir, 31 a 12.
- El resto no son relevantes ya que están comprendidos en la página almacenada en la tabla y a los efectos de la traducción no actúan.
- El Buffer de Traducciones actúa como una pequeña memoria cache, almacenando los pares de valores indicados, para las últimas traducciones, ya que una vez traducida la dirección de una página, si ésta contiene código el procesador seguirá ejecutando dentro de esa página de modo que recurrirá asiduamente a esa entrada del TLB. El mismo comportamiento se verifica para variables, buffers y demás elementos de un trozo de software. Se denomina Vecindad.



# Translation Lookaside Buffer (TLB)

- Los bits de control por lo general son los atributos de la página seleccionada, mas otros que no están documentados, pero siendo un cache, imaginamos mínimamente bits LRU para determinar cual es el elemento que debe ser desalojado al necesitarse una entrada para almacenar una nueva traducción estando el TLB lleno.
- El tamaño del TLB ha ido creciendo conforme se desarrollaron nuevos procesadores. Actualmente se tiene uno para código y otro para datos ubicados en la cache L1 de código y datos del procesador.
- Por otra parte como la paginación se organiza en base a tareas, cada tarea tendrá su propia estructura con lo cual el registro **CR3** cambiará de una tarea a otra. La escritura de un valor en el registro **CR3** flushea el contenido de la TLB (Excepto aquellas entradas que, como veremos, se setean como Globales)



# Extensiones de Memoria Física

- Con el procesador **Pentium Pro**, Intel inaugura una línea de procesadores IA-32 para servers, posteriormente continuada por el procesador **Xeon**. El **Pentium** por su parte queda destinado al segmento desktop .
- **Pentium Pro** introduce dos métodos para extender la capacidad de direccionamiento físico: Physical Address Extensions (PAE) y Page Size Extensions (PSE-36).
- Ambos son mutuamente excluyentes y se seleccionan mediante flags del registro **CR4**.
- PAE es en sí un modo de paginación (es el que se ha impuesto entre los desarrolladores de Sistemas Operativos). No obstante vale la pena un vistazo a la traducción basada en PSE-36.



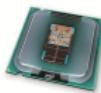
# Page Size Extensions (PSE-36)

- Se activa seteando el bit **CR4.PSE**. Es el bit 4.
- Debe asegurarse de tener **CR4.PAE = 0**, ya que ambos modos de extensión son mutuamente excluyentes.
- Habilita en el procesador 4 terminales de address adicionales:  $A_{35-32}$ . Esto extiende el bus de Address a 36 líneas, permitiendo manejar 64 Gbytes de memoria física.



# Page Size Extensions (PSE-36)

- La limitación de este modo es que el remanente de 4 Gbytes solo puede ser manejado en páginas de 4 Mbytes de tamaño.
- Con la evolución de esta arquitectura se activaron mas terminales de Address, y debido a la amplia aceptación de PAE, hay modelos de procesadores que no soportan PSE-36.
- Por lo tanto antes de activar PSE-36, lo recomendable es chequear previamente que el procesador soporte este modo. Esta comprobación se realiza mediante la instrucción **CPUID.01H:EDX.PSE[bit 3]=1**.



# Comprobación y activación de (PSE-36)

Este código comprueba el soporte del procesador al modo PSE-36 y su activación tomando los recaudos antes mencionados.

```
1  mov    eax,1          ;cpuid function
2  cpuid
3  test   edx, 8         ;bit 3 en 1?
4  jz     PSE_not_supported
5  mov    eax, cr4
6  test   eax, 0x20       ;bit PAE en '1'?
7  jnz   PAE_activo
8  or    eax, 0x10        ;bit 4 a '1'
9  mov    cr4, eax        ;PSE-36 activo
```



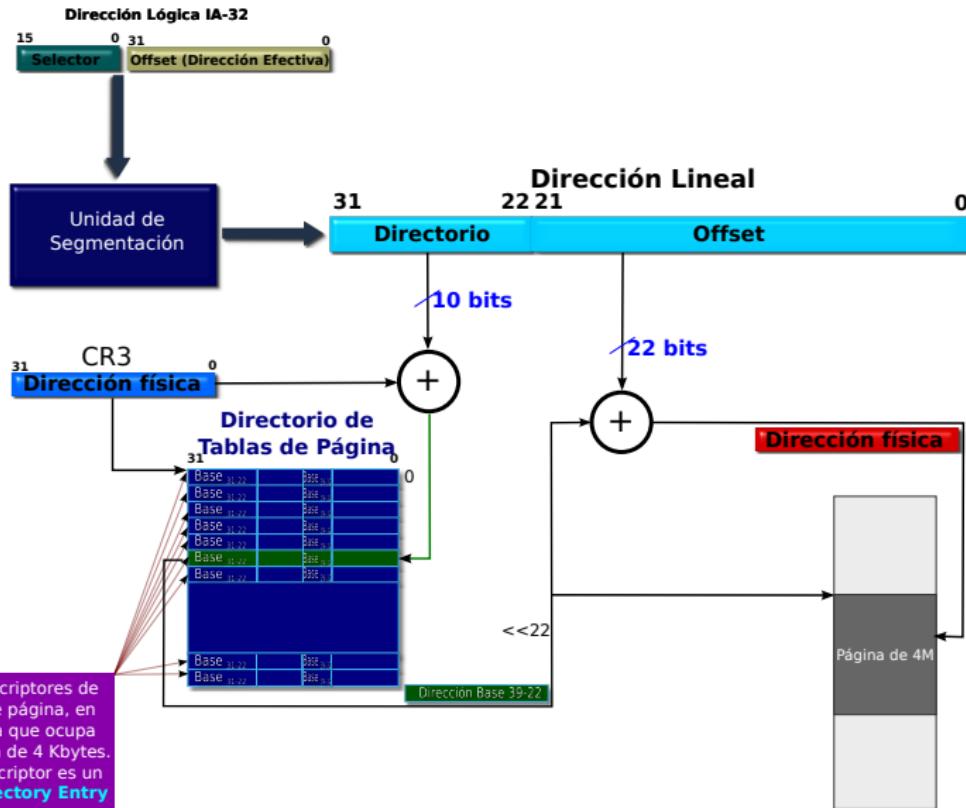
# Memoria física mas allá de 64 Gbytes

## Comprobando la cantidad de memoria física

- La cantidad de memoria física cambia de modelo a modelo.
- La instrucción CPUID.80000008H:EAX[7:0] es la manera indicada de determinar la cantidad de terminales de address que posee el procesador.
- Esta cantidad es el número binario contenido en el registro **AL** (**EAX**[7:0], coincide con este registro de 8 bits) a la salida de la CPUID invocada con **EAX** = 0x80000008.
- Intel denomina a este parámetro **MAXPHYADDR**.
- Si el procesador no soporta CPUID.8000008H, tiene a lo sumo 36 bits de direcciones (siempre que soporte PSE-36).



# Traducción con Páginas de 4 Mbytes



1024 descriptores de Tablas de página, en una tabla que ocupa una Página de 4 Kbytes. Cada Descriptor es un Page Directory Entry

# Traducción con Páginas de 4 Mbytes

## ¿Que cambia?

- La figura anterior muestra el esquema de traducción solo con el **DPT**, ya que en una página de 4 Mbytes los 22 bits menos significativos de la dirección base son '0'.
- Por lo tanto los 10 bits que en el sistema de 4 Kbytes se utilizaban como índice para la **PT** ahora no se necesitan. Se aprovecha para alojar allí los bits  $A_{39-32}$  de la dirección física.
- La cantidad significativa surge de la instrucción CPUID.80000008H.



# Traducción con Páginas de 4 Mbytes

## Precauciones

- Se sigue teniendo descriptores de 32 bits, ya que los bits adicionales de address se alojan en el espacio dejado por los bits  $A_{21-12}$ , que en una página de 4 Mbytes son siempre '0'.
- Cabe destacar que es posible diseñar un sistema de paginación mixto con páginas de 4 Kbytes y de 4 Mbytes. A continuación veremos como son los descriptores de página en detalle para cada caso y cuales son las limitaciones.



**1 Administración de memoria**

- Enfoque preliminar
- Gestión de la Memoria

**2 Como se organiza la memoria en procesadores x86**

- Modelo de memoria en Modo Protegido
- Modelo de memoria en Modo 64 bits

**3 Direcciones Lógicas y Lineales**

- Traducción de direcciones Lógicas

**4 Unidad de Segmentación**

- Selectores de segmento
- Descriptores de segmento de 32 bits

**5 Generación de la dirección Lineal (32 bits)****6 Modelos de segmentación de memoria**

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

**7 Paginación**

- Introducción
- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)
- **Formatos de descriptores de página**
- Paginación PAE
- Paginación IA-32e
- Niveles vs. Modos de paginación

**8 Paginación en ARMv7 Cortex-A y Cortex-R**

- Introducción
- Memory Management Unit

**9 Paginación en un Sistema Operativo Real: Linux**

# CR3: Descriptor de la Página que contiene el DPT

**CR3**

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Dirección física del Directorio de Páginas												Ignorados			P	P	W	Ignorados			D	C	T								

- Los bits 31 a 12 del registro contienen el page frame del (**DPT**).
- Esta dirección es física. O sea que el registro **CR3** contiene la dirección de RAM en donde comienza el **DPT**.
- En modo 64 bits, este registro tiene 64 bits. En el modo 32 bits, los bits 32 a 63 se ignoran.
- Bits de control de cache en tiempo de traducción.

**PWT** **Page-Level Write Through.** Establece el modo de escritura que tendrá la página en el Cache.

**PCD** **Page-Level Cache Disable.** Establece que una página integre el tipo de memoria no cacheable.



# Descriptores en el Directorio de Tablas de Páginas

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0								
Dirección física de la Tabla de Página																									P	S	I	G	N	A	P	C	W	T	U	R	/	W	P

Figura: Descriptor de la Tabla de Páginas de 4 Kbytes

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Bits 31 a 22 de la Dirección física del frame de la Página de 4M	Reservados deben ser 0	Bits 36 a 32 de la Dirección	P	A	T	Ignorados	G	P	S	D	A	P	C	W	T	U	/	S	R	/	W	P									

Figura: Descriptor de la Página de 4 Mbytes (PSE-36 activa)

- Ambos pueden coexistir en la misma tabla.
- En el primer descriptor, los bits 31 a 12 son los bits de la dirección física (el Page Frame) de la página que contiene la (**PT**).

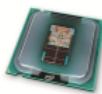


Una de las 1024 **PTE** de esa tabla describe la página que contiene la dirección de memoria solicitada por el procesador.

# Formato del descriptor de una Página de 4 Kbytes

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Dirección física del frame de la Página de 4 Kbytes	Ignorados	G	P A T	D	A	P C D	P W T	P U S	U R /W	R /W	P																				

- Hay entre 1 y 1024 de estos descriptores en cada una de las **PT** definidas en el **DPT**.
- Es el último nivel de traducción.
- Los bits 31 a 12, son el Page Frame de la página de memoria, es decir los 20 bits mas significativos de la dirección física donde ésta comienza (los 12 menos significativos son '0').



# Atributos de los descriptores

Son los mismos para todos los descriptores vistos y tienen el mismo significado.

**PS** **Page Size:** Existe solo en el **DPT**. Si es '0' la **PDE** corresponde a una **PT** de 4 Kbytes, y si es '1' a una página de 4 Mbytes.

**PAT** **Page Attribute Table:** Los MSRs **MTRR** definen y controlan el cache de diferentes zonas de memoria. A partir del Procesador Pentium III se dispone de este atributo que los complementa en base a páginas.

**G** **Global:** Si **CR4.PGE = 1** Tiene efecto la activación de la funcionalidad Global, que otorga ese carácter a la traducción de esa página almacenada en la TLB. La entrada no se flushea cuando se recarga el registro **CR3**.



# Atributos de los descriptores

- D **Dirty.** Indica que la página ha sido modificada (está "sucia"). El Sistema Operativo lo inicializa en '0', y se setea en forma automática en cada escritura en la página. El algoritmo de swap en el momento de desalojar una página de la memoria RAM, analiza este bit y no la copia al disco si no ha sido modificada, mejorando de este modo su eficiencia. Solo tiene sentido en descriptores de Página (de 4K o 4M). En las entradas del **DPT** que describen **TP** de 4 Kbytes se ignora ya que el Bit D existirá en el siguiente descriptor de la estructura.
- A **Accedido.** Se setea cada vez que la página es accedida. El Sistema Operativo puede contabilizar los accesos de modo de elaborar estadísticas de uso que permitan identificar cual es la página candidata a ser desalojada llegado el momento.



# Atributos de los descriptores

- U/S** User / Supervisor: Privilegio de la Página: '0' Supervisor (Kernel), y '1' Usuario. En general corresponden U/S = 0 a **DPL** = 00, y U/S = 1 al resto de los valores de **DPL**. El procesador chequea el **CPL** del segmento de código para autorizar o no el acceso a las páginas de acuerdo a la combinación de los valores de U/S de los diferentes descriptores de su estructura.
- R/W** Readable / Writable: Establece si la página es Read Only (0) o si puede ser escrita (1).
- P** Presente: Indica si la página está en la memoria ( $P=1$ ), generando una excepción #PF cuando se intenta acceder a una dirección de memoria que tiene al menos un descriptor con  $P=0$  a lo largo de la estructura de tablas. Cuando  $P = 0$ , el resto del contenido del descriptor se ignora.
- PCD y PWT** Idem registro **CR3**.



**1 Administración de memoria**

- Enfoque preliminar
- Gestión de la Memoria

**2 Como se organiza la memoria en procesadores x86**

- Modelo de memoria en Modo Protegido
- Modelo de memoria en Modo 64 bits

**3 Direcciones Lógicas y Lineales**

- Traducción de direcciones Lógicas

**4 Unidad de Segmentación**

- Selectores de segmento
- Descriptores de segmento de 32 bits

**5 Generación de la dirección Lineal (32 bits)****6 Modelos de segmentación de memoria**

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

**7 Paginación**

- Introducción
- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)
- Formatos de descriptores de página
- **Paginación PAE**
- Paginación IA-32e
- Niveles vs. Modos de paginación

**8 Paginación en ARMv7 Cortex-A y Cortex-R**

- Introducción
- Memory Management Unit

**9 Paginación en un Sistema Operativo Real: Linux**

# Características del Modo PAE

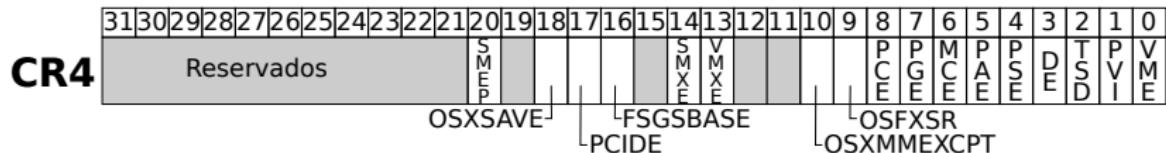
- Introducido como hemos dicho por el procesador Pentium Pro.
- Permite trabajar con páginas de 4 Kbytes o de 2 Mbytes, pudiendo particionar con cualquiera de los tamaños de páginas o incluso combinando ambos tamaños, el espacio físico completo.
- PAE evolucionó con la arquitectura y en la actualidad permite trabajar hasta con 52 bits de memoria física (hasta 4 Pbyte de RAM).
- Recordemos que la cantidad de bits de memoria Física se obtiene como resultado de CPUID.0x80000008, en el registro **AL**, y se denomina **MAXPHYADDR**.
- Si **MAXPHYADDR** < 52, los bits 51 y consecutivos en orden descendente, hasta el que corresponda al peso **MAXPHYADDR**, deben estar en '0'.



Es la base del modo de paginación IA-32e.

# Activación del Modo PAE

PAE se activa haciendo **CR4.PAE = 1**. Hemos nombrado varios bits del registro **CR4**. A continuación el layout de este registro.



Una vez activado, PAE permite, traducir una **dirección lineal** de 32 bits en una **dirección física** de 52 bits.  
Observar que de todos modos accedemos a un espacio lineal de 4 Gbytes tope en cada momento.



# Estructura de traducción del Modo PAE

**CR3**

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Dirección física de la Tabla de punteros a Directorio de Páginas																										Ignorados					

- En PAE el procesador arma una estructuras jerárquicas tres niveles.
- La base es siempre **CR3** (que como vemos difiere del layout para el modo 32 bits)
- El primer nivel es un array de cuatro punteros a Directorios de Tablas de Páginas.
- El registro **CR3** contendrá la dirección base de esta tabla de 4 punteros, **la cual debe estar alineada a 32 bytes**. Esta condición debe ser respetada **o el procesador generará una excepción**.



# Estructura de traducción del Modo PAE

## Tabla de Punteros de Directorio de Página

- La Tabla de Punteros de Directorio de Página (de ahora en mas **PDPT**), apuntada por **CR3**, consta de 4 entradas denominadas **PDPTEntry** (por Page Directory Pointer Table Entry)
- Cada **PDPTEntry** maneja el acceso a 1 Gbyte de memoria lineal.
- El procesador mantiene un set de 4 registros internos (no arquitecturales): **PDPTEntry0**, **PDPTEntry1**, **PDPTEntry2**, y **PDPTEntry3**.
- Estos registros mantienen el puntero a su respectivo **DPT** asociado, para agilizar la traducción de direcciones, tal como un cache.
- Se recargan desde sus respectivas copias en la memoria RAM cada vez que ésta altera su valor.
- El sistema trabaja con la versión RAM de la **PDTP**, el procesador debe releerlas para mantener actualizada esta cache interna.

# Cuando se regargan los 4 registros

- Si se ejecuta una instrucción cuyo operando destino es el registro **CR0**, o el registro **CR4** y como resultado de la cual se modifica uno o mas de los bits:

**CR0.CD** Cache Disable. '1' deshabilita el cache del procesador.

**CR0.NW** Non\_Write Through. Establece globalmente esta política de escritura. Solo tiene sentido si **CR0.CD** = 0.

**CR0.PG** Activa Paginación.

**CR4.PAE** Activa el modo PAE.

**CR4.PGE** Permite definir el uso de Páginas globales que se habilitan una a una con el bit **PG** de DPTE.

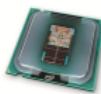
**CR4.PSE** Habilita o deshabilita el modo PSE-36

**CR4.SMEP** Habilita un modo de protección denominado **Supervisor Mode Execution Prevention**.



# Cuando se regargan los 4 registros

- Cuando se modifica el registro **CR3**, ya que debe buscarse de memoria el nuevo set de cuatro punteros que gestionará el espacio lineal de 4 Gbytes.
- Tal como veremos al abordar el manejo de Tareas, el registro **CR3** forma parte del contexto de ejecución que el procesador salvará y recuperará cuando llegue el momento.
- Algunas instrucciones de las extenciones de virtualización (VMX) motivarán también la carga de estos registros por parte del procesador.



# PAE: Traducción

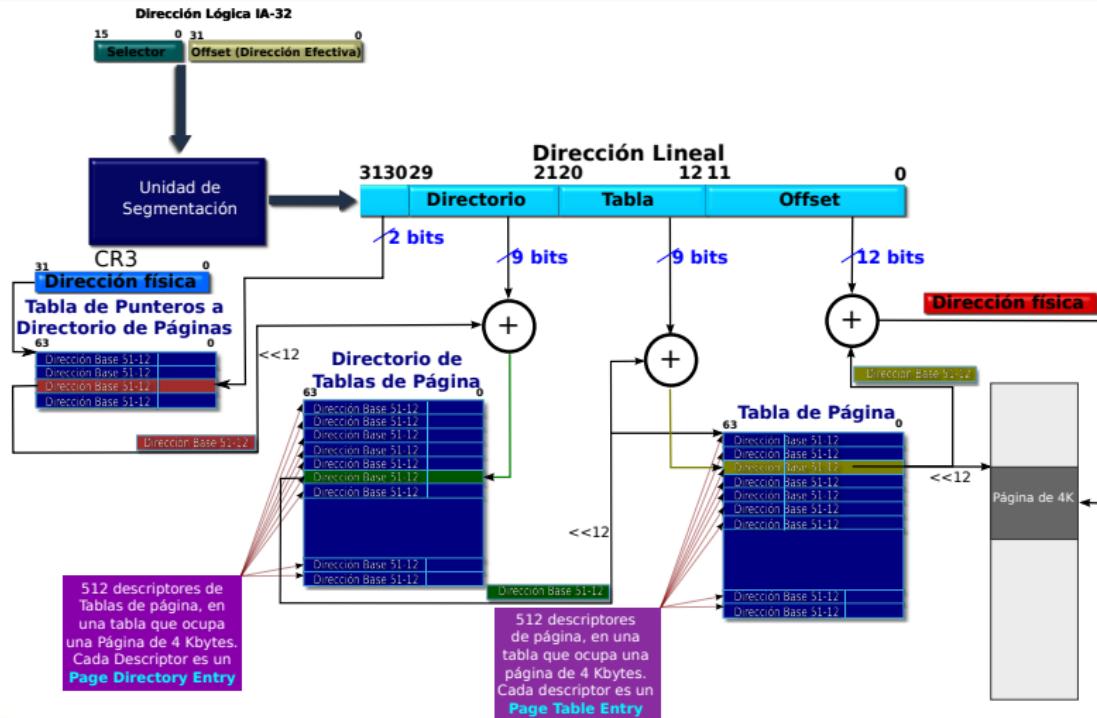
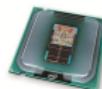


Figura: Mecanismo de traducción de 3 niveles con PAE activo y páginas de 4K



# PAE: Traducción

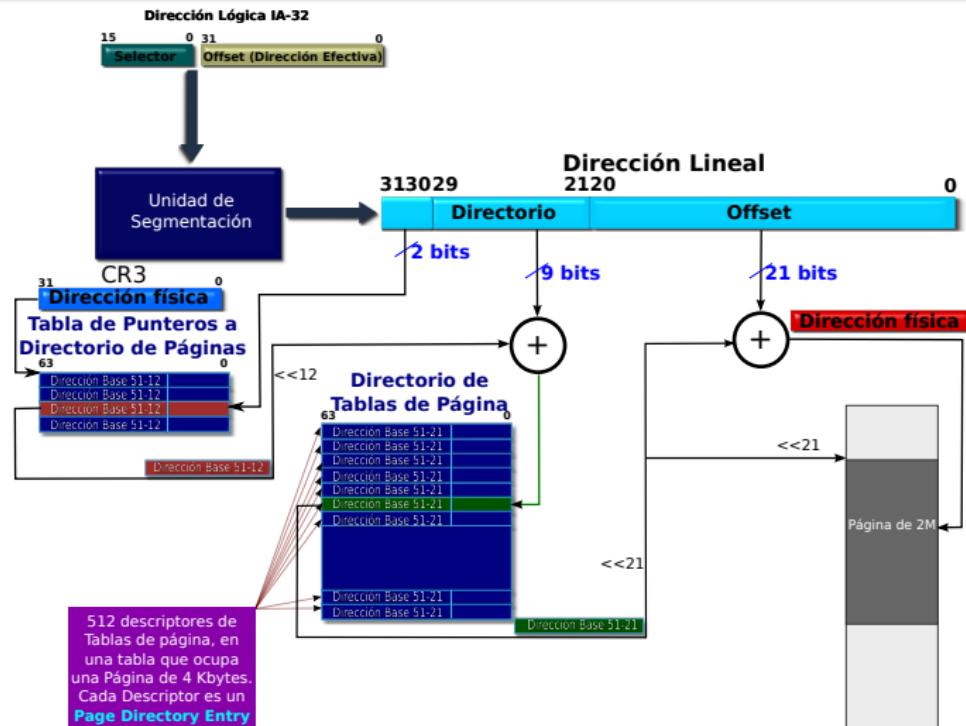


Figura: Mecanismo de traducción de 2 niveles con PAE activo y páginas de 2M

# PAE highlights

- Permite mapear páginas de 4 Kbytes o 2 Mbytes en cualquier parte del espacio físico.
- Soporta la cantidad de memoria física que fuese necesaria sin restricciones.
- Los descriptores de página ocupan en esta jerarquía el doble de tamaño (8 bytes).
- Por lo tanto en cada página física de 4 Kbytes caben 512 descriptores (la mitad respecto del Modo 32 bits).
- Se requieren 9 bits para indexar al descriptor buscado entre los 512 contenidos en la página.

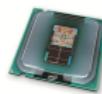


# Formato de los Descriptores

63 62 61 60 59 58 57 56 55 54 53 52 51 50 49 48 47 46 45 44 43 42 41 40 39 38 37 36 35 34 33 32											
Reservados	Dirección física Page Directory de 4 Kbytes <sup>1</sup>										
31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0											
Dirección física Page Directory de 4 Kbytes <sup>1</sup>	<table border="1"> <tr> <td>Ignorados</td> <td>Reservados (deben ser 0)</td> <td>P</td> <td>P</td> <td>Resrv</td> </tr> <tr> <td>C</td> <td>W</td> <td>D</td> <td>T</td> <td>deben ser 0</td> </tr> </table>	Ignorados	Reservados (deben ser 0)	P	P	Resrv	C	W	D	T	deben ser 0
Ignorados	Reservados (deben ser 0)	P	P	Resrv							
C	W	D	T	deben ser 0							

<sup>1</sup> Los Bits 51 a M (con M=MAXPHYADDR) deben ser '0' si M < 52. MAXPHYADDR se obtiene, en el registro AL como resultado de la instrucción CPUID.0x80000008.

**Figura:** Formato de una entrada de la Tabla de Punteros a Directorio de Páginas (PDPTE)



# Formato de los Descriptores

63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32		
X D	Reservados																									Dirección física del frame del DPT de 4 Kbytes <sup>1</sup>							
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0		
Dirección física de la Tabla del DPT de 4 Kbytes <sup>1</sup>																										Ignorados	P S	I G N <sup>2</sup>	A C D	P W T	P U S	R /W	P

<sup>1</sup> Los Bits 51 a M (con M=MAXPHYADDR) deben ser '0' si M < 52. MAXPHYADDR se obtiene, en el registro AL como resultado de la instrucción CPUID.0x80000008.

<sup>2</sup> En el Bit 6 **IGN** significa ignorado.

**Figura:** Formato de una entrada del Directorio de Páginas (DPTE), que describe una Tabla de Páginas de 4 Kbytes



# Formato de los Descriptores

63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
X D	Reservados																											Dirección física del frame de la Página de 2 Mbytes <sup>1</sup>			
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Dirección física del frame de Página de 2 Mbytes <sup>1</sup>	Reservados (deben ser 0)												P A T	Ignorados	G	P S	D	A	P C D	P W T	U S	R /W	P								

<sup>1</sup> Los Bits 51 a M (con M=MAXPHYADDR) deben ser '0' si M < 51. MAXPHYADDR se obtiene, en el registro AL como resultado de la instrucción CPUID.0x80000008.

**Figura:** Formato de una entrada del Directorio de Páginas (DPTE), que describe una Página de 2 Mbytes

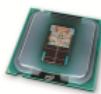


# Formato de los Descriptores

63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32			
X D	Reservados																								Dirección física del frame de la Página de 4 Kbytes <sup>1</sup>									
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0			
Dirección física del frame de la Página de 4 Kbytes																									Ignorados	G	P A T	D	A	P C D	P W T	U S	R / W	P

<sup>1</sup> Los Bits 51 a M (con M=MAXPHYADDR) deben ser '0' si M < 51. MAXPHYADDR se obtiene, en el registro AL como resultado de la instrucción CPUID.0x80000008.

**Figura:** Formato de una entrada del Tabla de Páginas (PTE), que describe una Página de 4 Kbytes



## 1 Administración de memoria

- Enfoque preliminar
- Gestión de la Memoria

## 2 Como se organiza la memoria en procesadores x86

- Modelo de memoria en Modo Protegido
- Modelo de memoria en Modo 64 bits

## 3 Direcciones Lógicas y Lineales

- Traducción de direcciones Lógicas

## 4 Unidad de Segmentación

- Selectores de segmento
- Descriptores de segmento de 32 bits

## 5 Generación de la dirección Lineal (32 bits)

## 6 Modelos de segmentación de memoria



- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

## 7 Paginación

- Introducción
- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)
- Formatos de descriptores de página
- Paginación PAE
- Paginación IA-32e**
- Niveles vs. Modos de paginación

## 8 Paginación en ARMv7 Cortex-A y Cortex-R

- Introducción
- Memory Management Unit

## 9 Paginación en un Sistema Operativo Real: Linux

# En 64 bits, la paginación lo es casi todo...

- Este modo se activa únicamente al ingresar el procesador al modo de trabajo IA-32e sub modo 64 bits.
- Los tres modos de Paginación dependen del estado de tres bits:

***CR0.PG*** Habilita Paginación

***CR4.PAE*** Habilita PAE

***IA32\_EFER.LME*** Habilita la Operación en modo IA-32e sub-modo 64 bits

- Este último al establecer el modo IA-32e, automáticamente habilita la paginación de 64 bits.



# En 64 bits, la paginación lo es casi todo...

Para cada uno de los modos los tres bits deben tener estas combinaciones:

- ① **Paginación de 32 bits.** Para ingresar a este modo se deben establecer los siguientes valores:  
***CR0.PG* = 1, *CR4.PAE* = 0, y *IA32\_EFER.LME* = 0.**
- ② **Paginación PAE.** Para ingresar a este modo se deben establecer los siguientes valores:  
***CR0.PG* = 1, *CR4.PAE* = 1, y *IA32\_EFER.LME* = 0.**
- ③ **Paginación de 64 bits.** Para ingresar a este modo se deben establecer los siguientes valores:  
***CR0.PG* = 1, *CR4.PAE* = 1, y *IA32\_EFER.LME* = 1.**



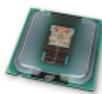
# Traducción en 64 bits

- Cuando se ingresa en el modo IA-32e el procesador genera direcciones lineales de 64 bits, si bien las microarquitecturas utilizarán direcciones de menor tamaño.
- Hasta el momento los procesadores que soportan el modo IA-32e utilizan direcciones lineales de 48 bits.
- Con esto se tienen 256 Tbytes (TeraBytes) de espacio lineal de direccionamiento.
- Para prevenir futuras ampliaciones Intel introdujo entre las funciones largas de la instrucción CPUID, una que informa la cantidad de bits que componen una **dirección lineal**, que en la documentación de CPUID aparece como **dirección virtual**, y la cantidad de bits que componen una **dirección física**, que no es mas que el parámetro **MAXPHYADDR** ya mencionado.



# Cantidades de bits en cada dirección

```
1 ;  
//  
2 ; Llamar a CPUID con EAX = 0x80000008  
3 ;  
//  
4 mov eax,0x80000008  
5 cpuid  
6 ; En este punto se tiene  
7 ; EAX 15–8 = Cantidad de bits soportados que conforman la  
; dirección virtual  
8 ; EAX 7–0 = Cantidad de bits soportados que conforman la  
; dirección física
```



# Estructuras de Paginación en 64 bits

## Raiz de la estructura

- Partimos del registro **CR3**. En el modo 64 bits su contenido depende de la habilitación o no del bit **CR4.PCIDE**.
- Este bit permite habilitar en el sistema cache la función **Process Context IDentifier (PCID)**, que permite a un procesador lógico cachear información desde múltiples espacios de direcciones lineales.
- Así el procesador lógico puede retener información en el cache aun cuando el software commute a otro espacio lineal de direccionamiento, por ejemplo cambiando el valor de **CR3**.
- Se usa solo en el modo 64 bits con cuatro niveles de paginación habilitados.

# Estructuras de Paginación en 64 bits

## Soporte a PCID

- Si un procesador soporta PCID luego de invocar CPUID.01h, el bit 17 del registro **ECX** es '1'.
- Una vez detectada su disponibilidad se habilita seteando el bit **CR4.PCIDE**
- Cada vez que el procesador genere una entrada en la estructura de la memoria cache y en la TLB, las asocia con el valor de PCID que figura en el campo homónimo del registro **CR3** (layout en el siguiente slide).



## Formato de CR3 en modo IA-32e

CR3

63						M <sub>1</sub>	M						39	38	37	36	35	34	33	32											
Reservados (deben ser 0)				Dirección física alineada a 4 Kbytes de la PML4																											
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Dirección física alineada a 4 Kbytes de la PML4												Ignorados				P	P	C	W	Ignor											

**Figura:** Layout del registro CR3 si CR4.PCIDE = 0

CR3

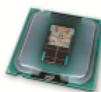
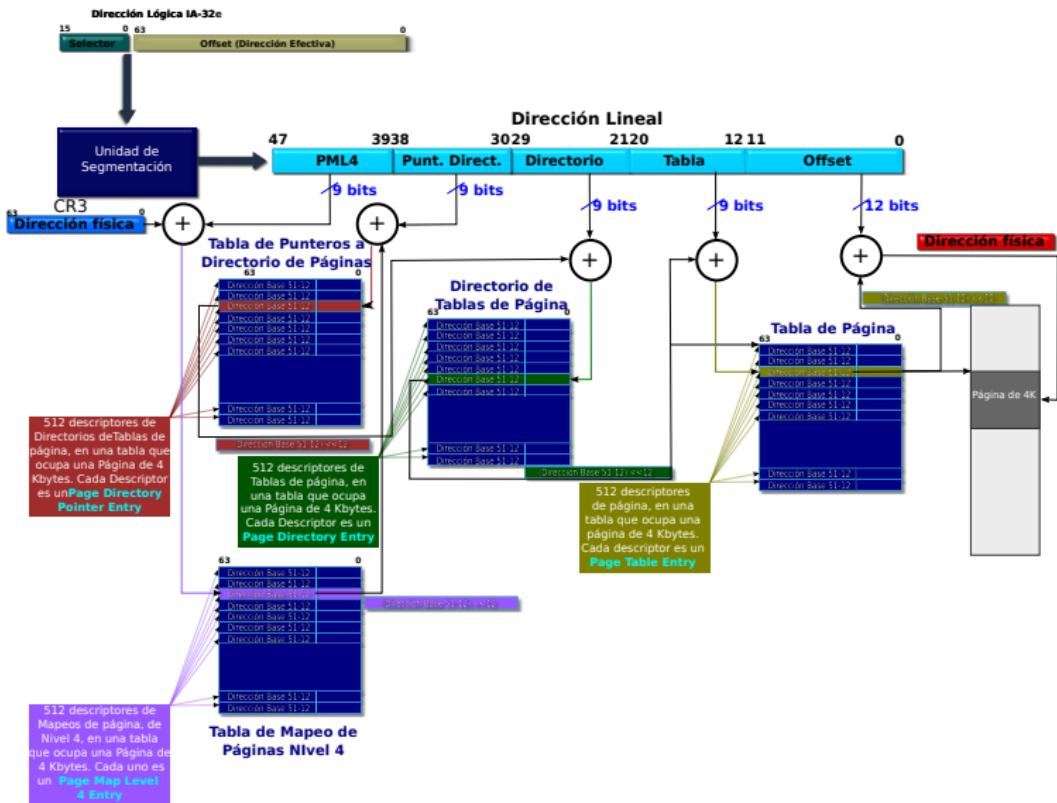
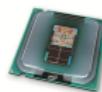
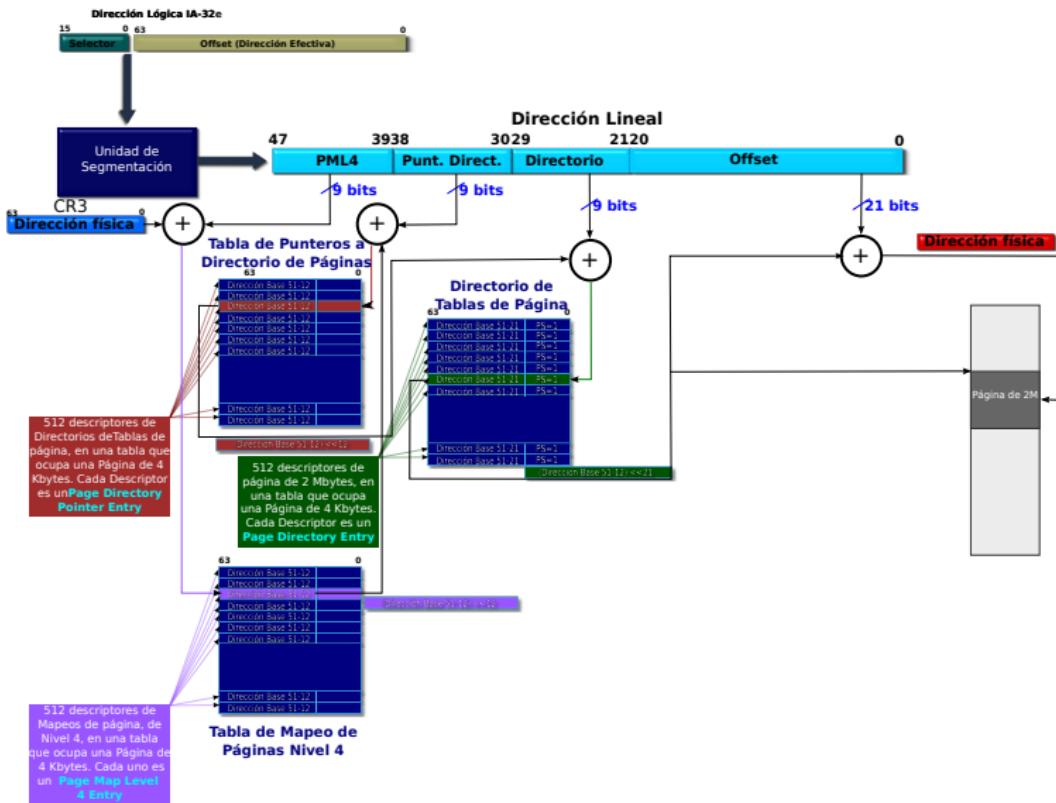


Figura: Layout del registro CR3 si CR4.PCIDE = 1

# Traducción de 4 niveles y páginas de 4 Kbytes

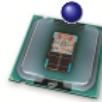


# Traducción de 3 niveles y páginas de 2 Mbytes

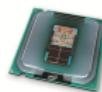
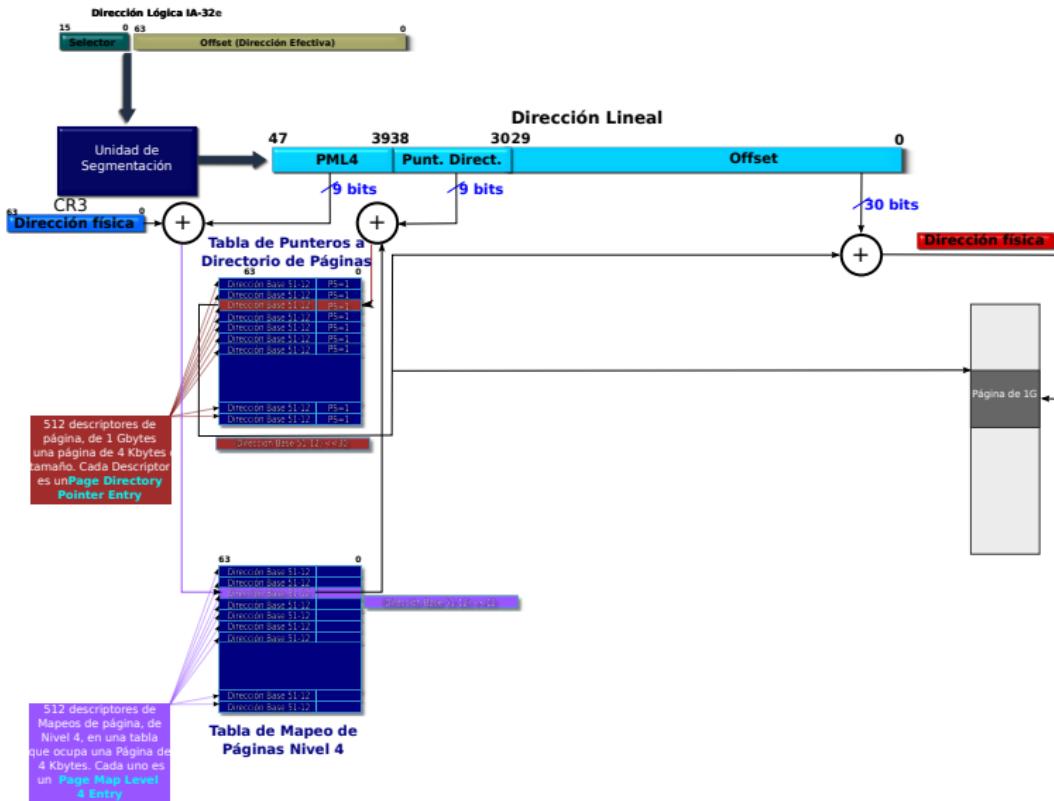


# Páginas de 1 Gbyte de tamaño

- El modo IA-32e tiene la posibilidad de trabajar con páginas de tamaño 1 Gbyte.
- Para ello emplea una estructura jerárquica de dos niveles, eliminándose el nivel de Directorio de Tablas de Página.
- Los 30 bits menos significativos de la dirección lineal son entonces el offset dentro de la página.
- La tabla de descriptores (PML4) permite direccionar hasta 512 tablas de Punteros a Directorios de Página, cada una de cuyas entradas contiene un descriptor de página cuyo atributo PS=1, y describe directamente una página alineada a 1 Gbyte y de ese tamaño.
- 250 Mega Páginas de 1 Gbyte, nos dá un espacio físico de 256 Peta Bytes.
- Para activar páginas de este tamaño es necesario antes chequear si el procesador lo soporta. La función 0x80000001 de CPUID, deja el bit 26 de EDX en '1'.

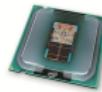


# Traducción de 2 niveles y páginas de 1 Gbytes



# Formato de CPUID Función 0x80000001

Bit	Name	Description when Flag = 1	Comments
31:30		<b>Reserved</b>	Do not count on the value.
29	Intel® 64	Intel® 64 Instruction Set Architecture	The processor supports Intel® 64 Architecture extensions to the IA-32 Architecture. For additional information refer to <a href="http://developer.intel.com/technology/architecture-silicon/intel64/index.htm">http://developer.intel.com/technology/architecture-silicon/intel64/index.htm</a>
28		<b>Reserved</b>	Do not count on the value.
27	RDTSCP	RDTSCP and IA32_TSC_AUX	The processor supports RDTSCP and IA32_TSC_AUX.
26	1 GB Pages	1 GB Pages	The processor supports 1-GB pages.
25:21		<b>Reserved</b>	Do not count on the value.
20	XD Bit	Execution Disable Bit	The processor supports the XD Bit when PAE mode paging is enabled.
19:12		<b>Reserved</b>	Do not count on the value.
11	SYSCALL	SYSCALL/SYSRET	The processor supports the SYSCALL and SYSRET instructions.
10:0		<b>Reserved</b>	Do not count on the value.



**1 Administración de memoria**

- Enfoque preliminar
- Gestión de la Memoria

**2 Como se organiza la memoria en procesadores x86**

- Modelo de memoria en Modo Protegido
- Modelo de memoria en Modo 64 bits

**3 Direcciones Lógicas y Lineales**

- Traducción de direcciones Lógicas

**4 Unidad de Segmentación**

- Selectores de segmento
- Descriptores de segmento de 32 bits

**5 Generación de la dirección Lineal (32 bits)****6 Modelos de segmentación de memoria**

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

**7 Paginación**

- Introducción
- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)
- Formatos de descriptores de página
- Paginación PAE
- Paginación IA-32e
- **Niveles vs. Modos de paginación**

**8 Paginación en ARMv7 Cortex-A y Cortex-R**

- Introducción
- Memory Management Unit

**9 Paginación en un Sistema Operativo Real: Linux**

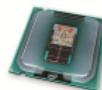
# Comparación entre los modos de paginación

La estructura General de Paginación varía de acuerdo al Modo de Paginación empleado. La Tabla muestra las características de los diferentes modos de paginación del procesador organizada por cada nivel de paginación de la estructura.

Paging Structure	Entry Name	Paging Mode	Physical Address of Structure	Bits Selecting Entry	Page Mapping
PML4 table	PML4E	32-bit, PAE	N/A		
		IA-32e	CR3	47:39	N/A (PS must be 0)
Page-directory-pointer table	PDPT	32-bit	N/A		
		PAE	CR3	31:30	N/A (PS must be 0)
		IA-32e	PML4E	38:30	1-GByte page if PS=1 <sup>1</sup>
Page directory	PDE	32-bit	CR3	31:22	4-MByte page if PS=1 <sup>2</sup>
		PAE, IA-32e	PDPT	29:21	2-MByte page if PS=1
Page table	PTE	32-bit	PDE	21:12	4-KByte page
		PAE, IA-32e		20:12	4-KByte page

**NOTES:**

- Not all processors allow the PS flag to be 1 in PDPTEs; see Section 4.1.4 for how to determine whether 1-GByte pages are supported.



# Resumen de cada Modo de Paginación

Paging Mode	PG in CR0	PAE in CR4	LME in IA32_EFER	Lin.-Addr. Width	Phys.-Addr. Width <sup>1</sup>	Page Sizes	Supports Execute-Disable?	Supports PCIDs?
None	0	N/A	N/A	32	32	N/A	No	No
32-bit	1	0	0 <sup>2</sup>	32	Up to 40 <sup>3</sup>	4 KB 4 MB <sup>4</sup>	No	No
PAE	1	1	0	32	Up to 52	4 KB 2 MB	Yes <sup>5</sup>	No
IA-32e	1	1	2	48	Up to 52	4 KB 2 MB 1 GB <sup>6</sup>	Yes <sup>5</sup>	Yes <sup>7</sup>

## NOTES:

1. The physical-address width is always bounded by MAXPHYADDR; see Section 4.1.4.
2. The processor ensures that IA32\_EFER.LME must be 0 if CR0.PG = 1 and CR4.PAE = 0.
3. 32-bit paging supports physical-address widths of more than 32 bits only for 4-MByte pages and only if the PSE-36 mechanism is supported; see Section 4.1.4 and Section 4.3.
4. 4-MByte pages are used with 32-bit paging only if CR4.PSE = 1; see Section 4.3.
5. Execute-disable access rights are applied only if IA32\_EFER.NXE = 1; see Section 4.6.
6. Not all processors that support IA-32e paging support 1-GByte pages; see Section 4.1.4.
7. PCIDs are used only if CR4.PCIDE = 1; see Section 4.10.1.



- 1 Administración de memoria
  - Enfoque preliminar
  - Gestión de la Memoria
- 2 Como se organiza la memoria en procesadores x86
  - Modelo de memoria en Modo Protegido
  - Modelo de memoria en Modo 64 bits
- 3 Direcciones Lógicas y Lineales
  - Traducción de direcciones Lógicas
- 4 Unidad de Segmentación
  - Selectores de segmento
  - Descriptores de segmento de 32 bits
- 5 Generación de la dirección Lineal (32 bits)
- 6 Modelos de segmentación de memoria
- 7 Paganación
  - Introducción
  - Unidad de Paganación - IA32
  - Paganación en IA-32 (32 bits)
  - Formatos de descriptores de página
  - Paganación PAE
  - Paganación IA-32e
  - Niveles vs. Modos de paginación
- 8 Paganación en ARMv7 Cortex-A y Cortex-R
  - Introducción
  - Memory Management Unit
- 9 Paganación en un Sistema Operativo Real: Linux



# Modos

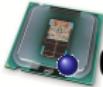
- En esta arquitectura de sistemas hay definidos dos modos de Paganación
  - short descriptor format** Permite acceder hasta 1 Tbyte de direccionamiento, aunque con una granularidad de 16 Mbytes.
  - long descriptor format** Equivalente al PAE en la arquitectura x86
- Lo primero que hay que hacer es detectar el soporte a paginación en cada procesador, mediante los registros del comprocesador. En este caso el registro **ID\_MMFR0** (Memory Model Feature Register 0)



31-28	27-24	23-20	19-16	15-12	11-8	7-4	3-0
Innermost Shareability	FCSE Support	Auxiliary Registers	TCM Support	Shareability levels	Outermost Shareability	PMSA Support	VMSA Supp

# Soporte VMSA

La clave es el campo VMSA Support

- **0b0000** - not supported (no paging)
- **0b0001** - implementación definida. Alguna MMU extraña en alguna parte
- **0b0010** - VMSAv6, Registros de tipo de cache y TLB . ARMv6 paging.
- **0b0011** - VMSAv7, soporte para remapeo y flag de acceso. ARMv7-A.
- **0b0100** - VMSAv7 con PXN bit suportado.
-  **0b0101** - VMSAv7, con PXN y long format descriptors. Soporta EPAE.

**1 Administración de memoria**

- Enfoque preliminar
- Gestión de la Memoria

**2 Como se organiza la memoria en procesadores x86**

- Modelo de memoria en Modo Protegido
- Modelo de memoria en Modo 64 bits

**3 Direcciones Lógicas y Lineales**

- Traducción de direcciones Lógicas

**4 Unidad de Segmentación**

- Selectores de segmento
- Descriptores de segmento de 32 bits

**5 Generación de la dirección Lineal (32 bits)****6 Modelos de segmentación de memoria**

- Segmentación en Modo IA-32e
- Implementación práctica de segmentación en un SO

**7 Paginación**

- Introducción
- Unidad de Paginación - IA32
- Paginación en IA-32 (32 bits)
- Formatos de descriptores de página
- Paginación PAE
- Paginación IA-32e
- Niveles vs. Modos de paginación

**8 Paginación en ARMv7 Cortex-A y Cortex-R**

- Introducción
- Memory Management Unit

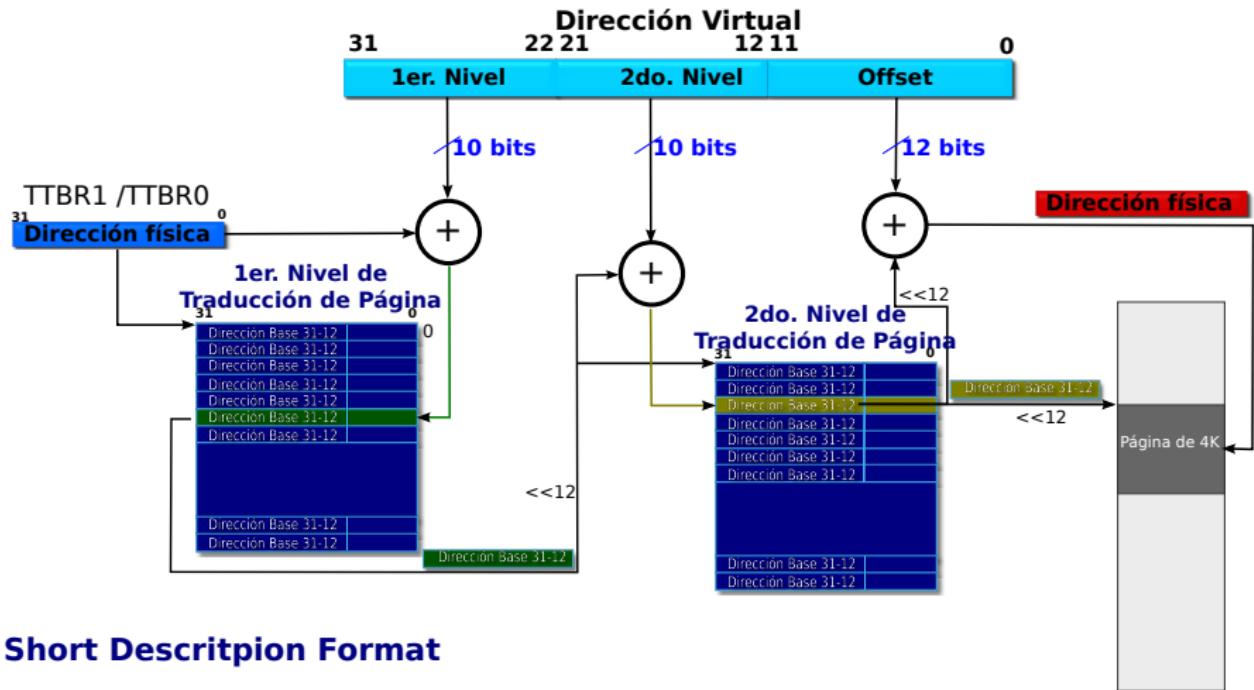
**9 Paginación en un Sistema Operativo Real: Linux**

# Modelo de Memoria en procesadores ARM

- Los procesadores ARM, manejan un espacio de direccionamiento flat de  $2^{32}$  bytes, que también puede ser considerado de  $2^{31}$  halfwords de 16 bits de ancho, o de  $2^{30}$  words de 32 bits
- La arquitectura de memoria, presenta funciones para:
  - Generación de excepciones cuando se accede a direcciones de memoria no alineadas.
  - Restricción del acceso a áreas de memoria específicas por parte de las aplicaciones.
  - Trasladar direcciones virtuales en direcciones físicas.
  - Alterar la interpretación de words de 32 y 16 bits como little endian o big endian.
  - Control de orden de acceso a memoria.
  - Control de los caches.
  - Sincronización del acceso a memoria compartida por parte de múltiples procesadores



# Estructura de Paginación General de un ARMv7



## Short Description Format



# Diferentes clases de entradas

Cada descriptor ubicado en uno u otro de los dos niveles se denomina genéricamente "Entry" por entrada, en referencia a cada entrada de la tabla que contiene un descriptor. De este modo los diferentes tipos de descriptores que podemos tener se clasifican en:

**Invalid o Fault Entry** Entrada e formato inválido. Un intento de acceso a ésta genera una Excepción.

**Page Table Entry** Apunta a una tabla de traducción de segundo nivel

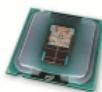
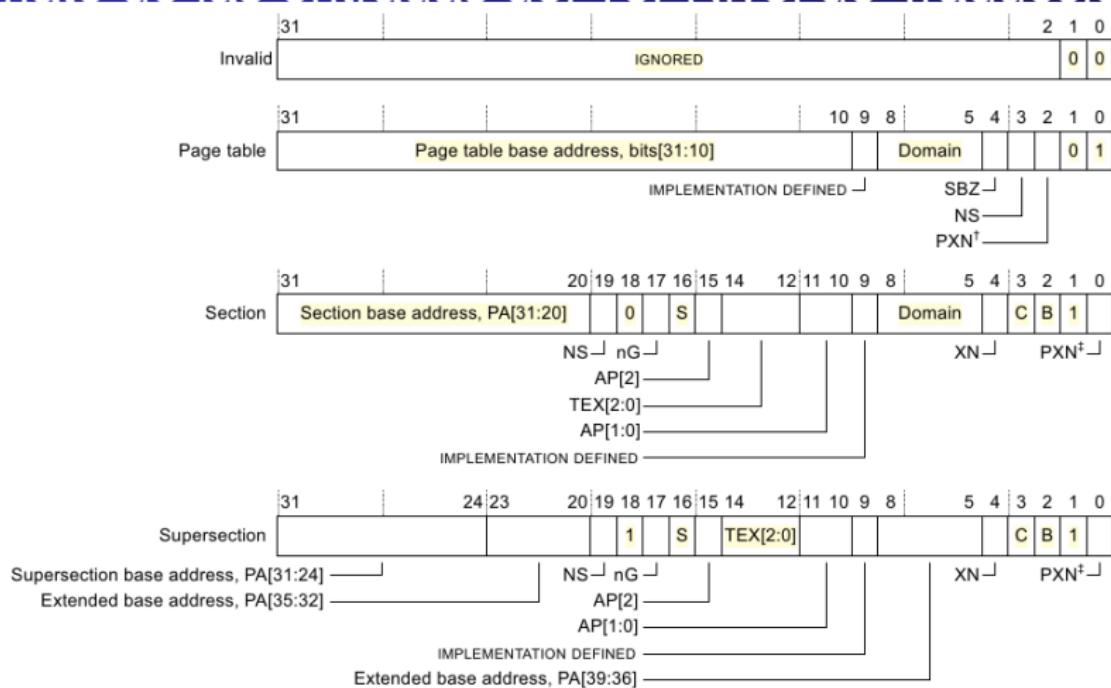
**Page Entry** Define en el segundo nivel de traducción los atributos de una página de memoria física de 4K o de 64 K.

**Section Entry** Define en el primer nivel de traducción los atributos de una sección de memoria física de 1 Mbyte de tamaño.

**Supersection Entry** Define en el primer nivel de traducción los atributos de una sección de memoria física de 16 Mbyte de tamaño.

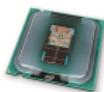


# Formato de las entradas del 1er Nivel de Traducción

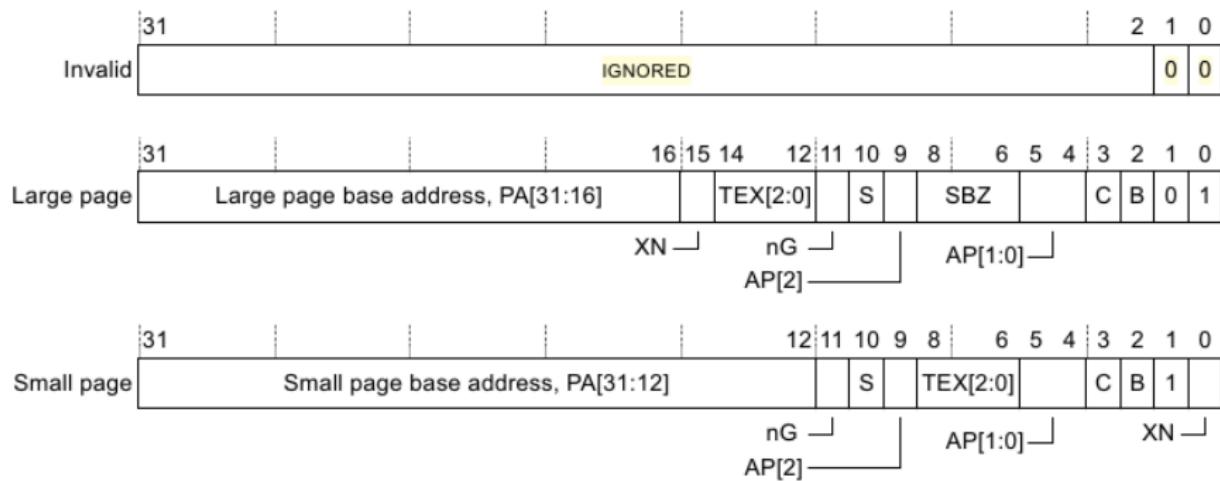


# Tipos de descriptores del 1er Nivel de Traducción

- Los bits 0 y 1, identifican el tipo de descriptor
  - 00 Descriptor Inválido. Acceder a un descriptor de este tipo genera una excepción de Traducción.
  - 01 El Descriptor contiene la dirección de una Tabla de Página de 2do. Nivel.
  - 10 De acuerdo al **bit [18]**, define una Sección (1Mbyte) o una Supersección (16Mbytes). Si el modelo de procesador soporta **Priviledge eXecute Never** bit, el bit **PXN** del descriptor debe estar en 0.
  - 11 Idem anterior pero el bit **PXN** del descriptor, debe estar en 1. En este caso la implementación soporta PXN



# Formato de las entradas del 2do Nivel de Traducción



# Tipos de descriptores del 2do. Nivel de Traducción

- Los bits 0 y 1, identifican el tipo de descriptor
  - 00 Descriptor Inválido. Acceder a un descriptor de este tipo genera una excepción de Traducción.
  - 01 El Descriptor contiene la dirección de una de Página Larga. Define un 64 Kbytes de memoria física, y sus atributos.
  - 1x El Descriptor contiene la dirección de una de Página Corta. Define un 4 Kbytes de memoria física, y sus atributos. En este formato el **bit [0]** es el bit **XN**.



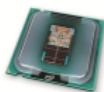
# Atributos de los descriptores (1er y 2do Nivel)

**Text[2:0],C,B** Atributos de región de memoria. Permiten definir los diferentes tipos de memoria, su cacheabilidad, posibilidad de remapeo, entre otros atributos.

**XN** eXecute Never bit. Impide (cuando es '1') que se ejecute código en esa página o sección siempre que la página tenga **Domain Client**. Un opcode fetch en una página con **XN = 1** genera una Excepción *Permision Fault*. No existe en la Page Table Entry (1er. Nivel de traducción).

**PXN** Priviledge eXecute Never bit. Cuando está soportado por la versión del procesador, se comporta como **XN**, pero si el opcode fetch se realiza desde PL1.

**S** Shareable bit. Indica si la página contiene una región de memoria compartida. Aplica a descriptores de sección o supersección en el 1er nivel o en descriptores de página corta y larga e el 2do nivel.



# Atributos de los descriptores (1er y 2do Nivel)

- NS** Non Secure bit. Si el procesador tiene activas las Extensiones de Seguridad, este bit indica en los accesos a memoria hechas desde el Estado Seguro, si la región de memoria accedida pertenece o no a un espacio de memoria definido como Seguro. Solo existe en el 1er nivel de traducción y afecta a todas las páginas del 2do. nivel derivadas de éste descriptor.
- nG** non Global bit. No existe en Descriptores de Tabla de Página. Indica como es tratada la traducción en la TLB de la dirección virtual a la física descripta por esta entrada. Si  $nG = 0$ , significa que la página es compartida por todos los procesos.



# Atributos de los descriptores (1er y 2do Nivel)

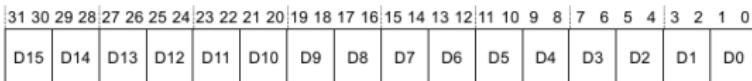
**Domain** Un Dominio es un conjunto de hasta 16 regiones de memoria que puede tener un proceso. Se definen mediante un campo de 4 bits solamente en Descriptores de Sección o de Tablas de Página. Un proceso soporta hasta 16 Dominios diferentes codificados en este campo. Cada dominio le otorga una condición sobre toda el área de memoria que lo compone, a saber:

No Access

Client

Manager

Se definen en el registro **DACR**, cuyo layout es:



Es decir que un proceso puede ser Manager de ciertas áreas de memoria de su dominio, cliente de otras y no tener acceso a otras.



# Atributos de los descriptores (1er y 2do Nivel)

**AP[2], AP[1:0]** Estos bits de permisos de accesos existen en todos los descriptores excepto en el de Tabla de Páginas que aparece en el primer nivel de traducción. Pueden trabajar en dos modos:

- **AP [2 : 1]** son dos bits de permisos de acceso, y **AP [0]** se puede utilizar como flag de Acceso. Esta opción se habilita con **SCTLR.AFE = 1**.

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0		
(0)				0			1	1				1		1	0	V	I	Z	0	0	0	1		1	1	C	A	M					
TE	TRE		EE		U	FI		WXN <sup>†</sup>		HA					RR		SW		B														
AFE	NMFI		VE					UWXN <sup>†</sup>																									
<b>AP[2], disable write access</b>				<b>AP[1], enable unprivileged access</b>				<b>Access</b>																									
0												0 <sup>a</sup>																					
0												1																					
1												0 <sup>a</sup>																					
1												1																					

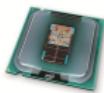


# Atributos de los descriptores (1er y 2do Nivel)

**AP[2], AP[1:0]** Estos bits de permisos de accesos existen en todos los descriptores excepto en el de Tabla de Páginas que aparece en el primer nivel de traducción. Pueden trabajar en dos modos:

- **AP [2 : 0]** son tres bits de permisos de acceso.

AP[2]	AP[1:0]	PL1 access	Unprivileged access	Description
0	00	No access	No access	All accesses generate Permission faults
	01	Read/write	No access	Access only at PL1
	10	Read/write	Read-only	Writes at PL0 generate Permission faults
	11	Read/write	Read/write	Full access
1	00	-	-	Reserved
	01	Read-only	No access	Read-only, only at PL1
	10	Read-only	Read-only	Read-only at any privilege level, deprecated <sup>a</sup>
	11	Read-only	Read-only	Read-only at any privilege level <sup>b</sup>



# Generalidades

- Linux es un sistema operativo multiplataforma, lo cual supone compilar para diferentes microprocesadores.
- Esto crea a obligación en los desarrolladores de código de emplear estructuras de programación flexibles y portables.
- No basta para ello simplemente escribir código en C, sino hacerlo para que este resulte suficiente para cumplir estos objetivos.
- Implementar un código suficientemente flexible para un procesador x86 en lo que a paginación se refiere por si solo se hace un interesante problema, que implica detenerse a pensar de que forma definir una única estructura que sirva para implementar Paginación de 32, bits, PAE, o IA-32e.
- En general todos los procesadores tienen una estructura de paginación que básicamente se encarga de traducir una **dirección virtual** (en los procesadores x86 llamada **dirección lineal**), en una **dirección física**, apta para enviar al exterior por el bus de direcciones.

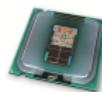
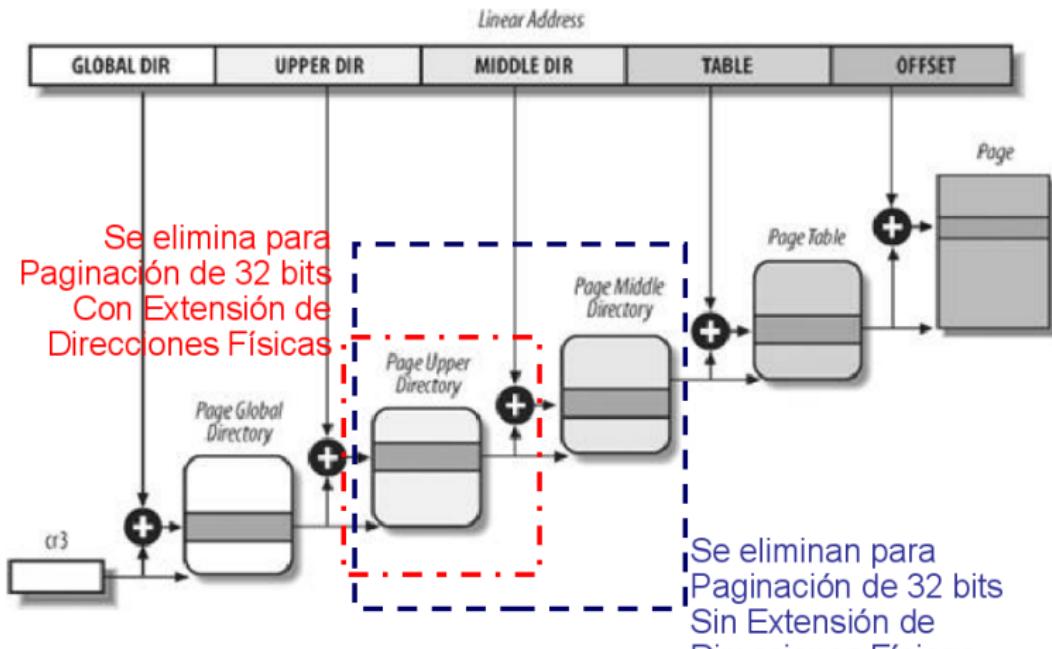


# Generalidades

- A diferencia de la administración de memoria por segmentación, que es prácticamente una marca registrada de los Procesadores x86, la administración de memoria por paginación es común a todos los procesadores que implementan multitarea y lidian con algún mínimo esquema de protección de memoria entre tareas.
- Hemos analizado la implementación de la paginación en los procesadores x86, en sus diferentes modos.
- Esto es lo que hace atractivo el estudio de esta familia de procesadores: No hay ninguna más compleja, y prácticamente en si misma presenta variantes para las que se requiere reunir otras varias arquitecturas diferentes.
- Habrá diferencias en la cantidad de bits de la **dirección virtual**, el tamaño de página, y otros detalles de implementación, en el mecanismo de traducción de cada arquitectura.
- Para implementar una estructura suficientemente flexible de programación, Linux se basa en un modelo genérico.



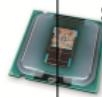
# Estructura de Paginación General de Linux



# Parámetros de Paginación para diferentes procesadores en Linux 32-bit

Arquitectura	PageSize	BitAddr	Niveles	Bits de cada campo
alpha	8 Kbytes	43	3	10 + 10 + 10 + 13
IA-64 (Itanium)	4 Kbytes	39	3	9 + 9 + 9 + 12
ppc64	4 Kbytes	41	3	10 + 10 + 9 + 12
sh64	4 Kbytes	41	3	10 + 10 + 9 + 12
Intel IA32	4 Kbytes	32	2	10 + 10 + 12
Intel IA32 PAE	4 Kbytes	32	3	2 + 9 + 9 + 12
Intel® 64	4 Kbytes	48	4	9 + 9 + 9 + 9 + 12
ARM CORTEX A	4 Kbytes	32	2	10 + 10 + 12

Así es que para cada arquitectura un conjunto de macros permiten definir la cantidad de bits de cada acampo de la **dirección virtual** particionada en 4 niveles en la Figura anterior, pudiendo colapsar uno o hasta dos campos intermedios simplemente poniendo 0 como su valor a la marco que define la cantidad de bits de ancho de ese campo.



# Lineamientos para Administración de la memoria

Se trata de optimizar el uso de la memoria asignando a cada proceso y al mismo kernel solo la memoria necesaria, y liberándola ni bien haya finalizado su uso.

- ① El kernel se asigna de modo permanente un área de memoria para su código y sus estructuras de datos estáticas
- ② El resto se denomina *memoria dinámica*, y consiste en un recurso fundamental, tanto para los procesos como para el mismo kernel.
- ③ Como consecuencia de los dos ítems anteriores, la correcta administración de la *memoria dinámica* impacta directamente en la performance del sistema.



# Lineamientos para Administración de la memoria

Las distribuciones de Linux de 32 bits trabajan con páginas de 4 Kbytes solamente (aún las que implementan PAE). Pesaron en la decisión los siguientes factores que se señalan como cruciales.

- El algoritmo de swaping es mas simple
- Si bien las transferencias de disco se hacen en múltiplos enteros de los tamaños de páginas de 4 Kbytes, lo cual permitiría emplear tamaños de páginas grandes, las transferencias de disco a memoria de menor tamaño son mas eficientes.



# Detalle del Page Fault handler

